

EMERGENCY MANAGEMENT INFORMATION AND TECHNOLOGY

HEARINGS BEFORE THE SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT OF THE COMMITTEE ON SCIENCE AND TECHNOLOGY U.S. HOUSE OF REPRESENTATIVES NINETY-SEVENTH CONGRESS FIRST SESSION

SEPTEMBER 29, 30, 1981

[No. 55]

Printed for the use of the
Committee on Science and Technology



U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1981

88-582 O

H701-25

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey	LARRY WINN, Jr., Kansas
GEORGE E. BROWN, Jr., California	BARRY M. GOLDWATER, Jr., California
JAMES H. SCHEUER, New York	HAMILTON FISH, Jr., New York
RICHARD L. OTTINGER, New York	MANUEL LUJAN, New Mexico
TOM HARKIN, Iowa	HAROLD C. HOLLENBECK, New Jersey
MARILYN LLOYD BOUQUARD, Tennessee	ROBERT S. WALKER, Pennsylvania
JAMES J. BLANCHARD, Michigan	EDWIN B. FORSYTHE, New Jersey
TIMOTHY E. WIRTH, Colorado*	WILLIAM CARNEY, New York
DOUG WALGREN, Pennsylvania	MARGARET M. HECKLER, Massachusetts
RONNIE G. FLIPPO, Alabama	F. JAMES SENSENBRENNER, Jr., Wisconsin
DAN GLICKMAN, Kansas	VIN WEBER, Minnesota
ALBERT GORE, Jr., Tennessee	JUDD GREGG, New Hampshire
ROBERT A. YOUNG, Missouri	RAYMOND J. McGRATH, New York
RICHARD C. WHITE, Texas	JOE SKEEN, New Mexico
HAROLD L. VOLKMER, Missouri	CLAUDINE SCHNEIDER, Rhode Island
HOWARD WOLPE, Michigan	JIM DUNN, Michigan
BILL NELSON, Florida	BILL LOWERY, California
BERYL ANTHONY, Jr., Arkansas*	
STANLEY N. LUNDINE, New York	
ALLEN E. ERTEL, Pennsylvania	
BOB SHAMANSKY, Ohio	
RALPH M. HALL, Texas	
DAVE McCURDY, Oklahoma	
MERVYN M. DYMALLY, California	

HAROLD P. HANSON, *Executive Director*

PHILIP B. YEAGER, *General Counsel*

REGINA A. DAVIS, *Administrator*

GERALD E. JENKS, *Minority Staff Director*

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

ALBERT GORE, Jr., Tennessee, *Chairman*

BOB SHAMANSKY, Ohio	ROBERT S. WALKER, Pennsylvania
HAROLD L. VOLKMER, Missouri	MANUEL LUJAN, Jr., New Mexico

*On assignment to Budget Committee for 97th Congress.

CONTENTS

WITNESSES

September 29, 1981:

William O. Baker, chairman emeritus, Bell Laboratories, Murray Hill, N.J.....	Page 5
Maj. Gen. Bennett L. Lewis, Executive Deputy Director, Federal Emergency Management Agency, accompanied by Charles Girard, Associate Director (designate), Resource Management and Administration, and Bruce J. Campbell, Assistant to the Associate Director for Information Resources Management.....	23
Robert D. Vessey, director, disaster services, American Red Cross, and president, National Voluntary Organizations Active in Disaster.....	39
Richard B. Foster, Director, Strategic Studies Center, SRI International....	47
Francis P. Hoerber, president, Hoerber Corp.....	79
Stephen J. Lukasik, Chief Scientist, Office of Science and Technology, Federal Communications Commission.....	100

September 30, 1981:

Thomas G. Belden, consultant, Rockville, Md.....	129
Robert E. Kahn, Director, Information Processing Techniques Office, Defense Advanced Research Projects Agency, Arlington, Va.....	166
Maj. Gen. Charles A. Ott, Jr., Director, Division of Emergency Services, Department of Emergency and Military Affairs, State of Arizona, accompanied by Milton L. Deeever, president, Comtech Data Corp.....	186
Charles K. Allen, director, public affairs and safety, city of Plainfield, N.J.....	224
George M. Hicken, Project Manager, coins, National Security Agency.....	243
James W. Morentz, Jr., president, Research Alternatives, Inc.....	268
Robert Kupperman, executive director, Center for Strategic and International Studies.....	296

EMERGENCY MANAGEMENT INFORMATION AND TECHNOLOGY

TUESDAY, SEPTEMBER 29, 1981

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
Washington, D.C.

The subcommittee met, pursuant to call, at 9 a.m., in room 2318, Rayburn House Office Building, Hon. Albert Gore, Jr. (chairman of the subcommittee) presiding.

Mr. GORE. The subject of disasters is not one that many of us care to dwell on. Earthquakes, fires, assassinations, terrorist attacks, and nuclear meltdowns are the stuff of Hollywood, and we like to keep it that way. As a result of this out-of-sight, out-of-mind ethic, our society is often ill equipped to deal with emergencies when they do arise. Out of neglect, we fail to bring to bear either the technology or the management capability needed to respond quickly and effectively to the demands of stress situations.

On March 30 of this year, all of us were shocked by the assassination attempt on the President of the United States. Partly as a result of that attempt, Mr. Richard Beal, Special Assistant to the President for Planning and Evaluation, and I began a dialog on the problems involved in keeping the nerve centers of Federal, State, and local governments going during situations like that. Like most Americans, I perceived that even our most veteran and skilled officials seemed ill equipped informationally to deal with the developing situation. In early May, with the assistance of the Congressional Research Service, I convened a group of some of the most distinguished Americans in the field of emergency management to discuss how we could make the American people aware of the difficulties we face during emergencies, and how we could begin to face up to the problems in management and communications that result. Our hearings over the next 2 days are the first step.

It is not the Subcommittee's intention to unduly alarm anyone. But during the hearing, we will hear about a variety of disasters that are not only plausible, but in some cases quite likely to happen at some point. We shall see that we are ill prepared to deal with some of these problems; and that we ought to quickly do something about the situation. For example it is becoming increasingly clear that our current national telecommunications network is insufficiently secure. This system is a vital part of our disaster preparedness and response; we must remedy the situation.

While I applaud the increased activism of the Federal Emergency Management Agency, I continue to be skeptical of that Agency's

ability to adequately deal with other Federal agencies that have important responsibilities during crises, and to adequately coordinate the Government's response in nonmilitary disasters. Anyone who was connected with the Three Mile Island incident—a mild event in the range of things we will hear about today—knows that FEMA has a long way to go before it can adequately handle crises.

Part of the problem in emergency management may stem from our divided system in which military and civilian disaster experts have operated. We need to take advantage of the expertise that we have developed in the national security arena to deal with natural disasters. We need to see whether we can develop in our civilian managers the sensitivity to training for emergency situations and to giving priority to simulation and training in their regular work.

Most importantly, we need to see how we can take advantage of the technology that is already on the shelf to upgrade our emergency management systems around the country.

We are fortunate to have with us over the next 2 days a group of people who form the leadership cadre in thinking and acting on disasters in the United States. I look forward to discussing the issues with them in this forum, and then moving forward together in a bipartisan effort to think about the unthinkable and prepare ourselves for the future.

At this time, I would like to read a letter from Mr. Richard Beal, expressing the administration's support of this hearing and, indeed, the entire undertaking:

Attached is a statement I have prepared for your committee hearings on Information Technology and Emergency Management scheduled for later this month and next month. This is to augment the earlier material we provided Robert Chartrand in conjunction with the roundtable discussions on the same subject held in May of this year.

Following discussions with Gen. Louis Giuffrida, Director of the Federal Emergency Management Agency (FEMA), it was decided that my testimony might be redundant. Therefore, it was felt that he should properly represent the administration in providing your subcommittee with information which is critical to this very important area. My attached remarks should complement those of General Lewis, the FEMA participant in the hearings.

I am going to ask, along with my colleague, Mr. Winn, that we put Mr. Beal's statement in the record.

[The prepared statement of Richard S. Beal follows:]

ATTACHMENT

STATEMENT OF DR. RICHARD S. BEAL
FOR HEARINGS ON INFORMATION TECHNOLOGY
AND EMERGENCY MANAGEMENTCOMMITTEE ON SCIENCE AND TECHNOLOGY
SUB-COMMITTEE ON INVESTIGATIONS AND OVERSIGHT

President Ronald Reagan took office with a mandate from the electorate to bring about major changes in the Federal Government. This mandate called for making better uses of resources available to the Government, as well as for narrowing the scope of Government to a more appropriate level of involvement in peoples lives. Of necessity in carrying out this mandate is ensuring that technology advances in all fields are developed and applied in whatever activity the Government engages in.

As Special Assistant to the President for Planning and Evaluation I have made efforts to ensure that consideration is given to the application of modern technology to the generic field of planning, as well as to several specific areas of planning which truly support the making of "life and death" decisions. The fields of emergency management and crisis planning are of such urgency. The President has instructed the Federal Emergency Management Agency (FEMA), under the direction of General Louis Giuffrida, to make special efforts to ensure that this Administration is properly planning for the entire range of hazards that confront us. And, the Administration fully supports General Giuffrida in his application of science and technology to the policies, programs and priorities of that Agency. FEMA will have direct access to the White House for current and short-range emergency management planning and operations as well as for the medium and long-range planning necessary to ensure that the White House is able to immediately respond to future potential major emergencies. We would be remiss if we were not preparing for both types of occurrences.

General Giuffrida, in his remarks, will provide detailed information about the specific actions he and his staff have already undertaken in conjunction with the White House staff to ensure that these directives are carried out. Further, he will most certainly comment on how advanced information technology is being applied and administered in FEMA for aiding both planning and operational decision making associated with emergency management.

The Administration has been most concerned about the lack of effective applications of science or technology to the field of emergency management that it found upon taking office. Special efforts have been made to ensure that ground is made up as rapidly as possible. We in the Office of Planning and Evaluation will work with the leadership in FEMA, and support them to the extent possible in continuing this critical task.

Thank you for the opportunity to provide this statement of support to your hearings. The President feels these to be of vital importance.

BEST COPY AVAILABLE

Mr. GORE. I might say that the subcommittee has greatly enjoyed working with Mr. Beal, who has provided a focus within the White House for a sustained, concentrated effort of the Government's performance in this area.

I am pleased to recognize my senior colleague, the ranking member of the Science and Technology Committee, Mr. Larry Winn.

Mr. WINN. Thank you, Mr. Chairman.

Mr. Chairman, I am pleased to be here today as we open this first day of hearings on the subject of Federal emergency management and response. I am sorry to say that the gentleman from Pennsylvania, Mr. Walker, who is the ranking Republican on this subcommittee, is unable to be with us this morning because of a conflict in his schedule. However, he has had a strong interest in this area and will be here for the next hearing.

Disaster can strike at any moment and at any place. In my part of Kansas we face the threat of tornadoes. In parts of California there is the constant threat of earthquakes. The gulf coast is often threatened by hurricanes. Fire and flood take dozens of American lives each year.

The focus of our hearings will be on what is the proper role of the Federal Government in disaster recovery planning and in management information to aid disaster recovery. We want to determine what the current state of the art is in high technology and how that technology can be applied to disaster recovery. We have invited a distinguished group of witnesses to discuss with us both the technological problems involved and the proper mix of Federal efforts, State and local contributions, and the role of American industry in this vital area.

Disaster recovery operations nearly always involve a close partnership among Federal, State, and local governments, and private sector organizations. The exact relationship is often an evolving one which depends on both the scope and nature of the disaster involved. We wish to examine the nature of that relationship, ways to improve it, the means of establishing effective communications among the partners, and the proper role of new technology in disaster recovery.

I am pleased to say that this effort is not only a bipartisan one within this committee, but it is also a joint venture with the Reagan administration. We all see that there are important problems here, and we want to work cooperatively to find solutions. In that regard we had hoped to be joined today by Dr. Richard S. Beal, the Special Assistant to the President for Planning and Evaluation. He was unable to come in person, but he has submitted a short statement which I would like to ask unanimous consent to incorporate in the record at this point.

Mr. GORE. Without objection we will do that.

Mr. WINN. I thank you, Mr. Chairman, and I want to congratulate the chairman of the subcommittee for holding these hearings and I look forward to the total report and the hearing information that has been submitted by the many fine witnesses that we will hear from in the next few days.

Thank you, Mr. Chairman.

Mr. GORE. Thank you.

I am quite optimistic that we will get something accomplished in these hearings.

Our first witness is a most distinguished one. We are pleased to have Dr. William O. Baker, chairman emeritus of Bell Laboratories, former president of Bell Laboratories. He has served as a high-level adviser to the National Science Foundation, National Security Agency, President's Science Advisory Committee, and I could go on and on. He is well known in this field and we are most pleased to have him as our leadoff witness.

Dr. Baker, welcome to you, and I do not know of anyone who could get us off to a better start in these 2 days.

**STATEMENT OF WILLIAM O. BAKER, CHAIRMAN EMERITUS,
BELL LABORATORIES, MURRAY HILL, N.J.**

Dr. BAKER. Thank you, Mr. Chairman. Good morning, gentlemen, ladies.

We, of course, recognize in these wise reviews of emergency planning and action, you will be dealing with all kinds of resources. One thinks, as the chairman has already suggested, of food, water, shelter, and medicine, the mobilization of those survival elements. The one we shall report on presently is less tangible, and the subcommittee has chosen, I think, with skill, to point to the problems of information communications. Those problems underlie, we guess, the technology and science of all emergency actions. The common element there is words, a commodity of some complexity.

The situation in emergencies is often summarized by a Yankee episode of some years ago when in a town meeting they were listening to a long and involved discourse on various complicated civic matters. One Yankee turned to another and said, "What is he talking about?"

And the other one said, "He don't say."

Well, this is what happens very quickly under stress and emergency conditions, and I should like to record briefly on how modern science and technology are influencing the handling of words, primarily. We shall look, if someone is willing, look at a few visuals as to what the national capabilities for managing information generally may be. We remind ourselves, as the chairman has pointed out, there is a national communications network, the largest connected machine so far built, but one which depends heavily for its reliability on a very great range of redundancy. This machine that our colleagues in FEMA are dealing with very thoughtfully has all kinds of technology operations such as radio, satellites, cables, and all the rest, but one has to emphasize that in emergencies, although this system is quite capable of handling data in any desired dimension, it gets largely words which are distributed in this particular case through the Bell System, but there are hundreds of other independent and connected communications systems in the Nation. It gets distributed through telephones primarily in this case about 150 million beyond the 132 million of this particular counting. Those are activated mostly with words.

They get interconnected, of course, by a huge number of loops that link to switching centers. Here is where a great deal of the emergency power resides; that is, the ability to use alternate routes

and to have duplicate systems. The new technique of CCIS, the interoffice signaling, is a highly valuable additional resource for that.

The inputs to that network which would be the primary feature of information handling, are, of course, very diverse and include primarily the voices from the telephone some of the graphics and the computer resources from tapes and other inputs. They go through an equally diverse set of media such as high-capacity cables, satellite links, and more conventional wires and cables through to, of course, the decoding at reception points which may involve visual facilities, computer reception, and so forth.

In the face of that, our capacity is going up steadily in the Nation and, of course, has taken an enormous leap from the use of photonics; those need to be counted in as we get to the next stage of communications. Photonics are over light beams.

We have to be cognizant that even in the home what would be involved in real disaster events. A great range of information handling is available or oncoming. These can involve sensors and systems for links with computers directly, visuals thus activated, file systems, but we remain sure that the word inputs are still going to be dominant.

Those, as we said, go out over these media from wires to cables to microwaves to satellites, and it is a diversity that gives us some security.

The progress in this field is rapid. Here is a millimeter-wave Earth satellite antenna. We can expect these in one form or another to come onto roofs and mobile systems and the like.

So, the satellites, instead of the very diverse broadcast which is in use now, satellites are in construction which will send these to very specific areas of the Nation, of the continent, and we will do a certain amount of switching in space so that we have this growing capability of redundancy and of diversity for emergency reaction.

These are areas, examples where a single satellite can have separate and identified messages.

The theme through this summary is that up to now we have depended on a very small part of the electromagnetic spectrum for all the handling of words and everything else in communication processing. But with the advent of photonics, the development of the laser, we spread this by many orders of magnitude. So the Nation has now a source for information management that is not two or three times but a million and a thousand million times what it has had up to now, since we can operate through the light range and continually through the infrared and up to microwaves and the present frequency ranges. Those are capacities for handling words and other information.

The whole essence of our summary, though, is in this diagram which says that any knowledge, words, visions, diagrams, images, anything else, turns out and can be coded completely and fully, the full information content represented by a digital system which is a set of zeroes and ones, used to sample an amplitude and the climb of a wave, which is a voice wave in this instance. It is some form of this which has to be assured and managed during emergencies to make the national reaction that is desired.

This information, which may be all these subtle words, are very simple ones; as we are going to see in a couple of minutes can be identified by zeroes, or an absence of a 1. This is the essence of all information in all modern computers and in modern information handling systems and an alternate form for communication systems. That alternate form, where we have in this Nation now a network which will handle both the analog and digital systems, is a source of great strength, Mr. Chairman, but one that is not fully mobilized as yet.

The next shows that this kind of assignment of 0's and 1's can be applied to written text, spoken words, of course, the alphabet in English takes about 5 bits per letter, the weather map, the image of the weather, onset of hostilities and whatever.

One of the impulses which gives a 1 is shown here. This 1 is one-billionth of a second in duration. There can be 1 billion in a second, or correspondingly, 1 billion 0's, which is the absence of the pulse. This brings us to our dilemma this morning, which is that words are put in and taken out by human beings and other things are understood by human beings at about 40 of these per second, but here it is possible to generate perhaps 1 billion per second, and we want to be able to do that in generating information, and that is where the human beings can relate to.

Small dots here are the peak-a-second pulses which are the laser beams, 1 million bits per second. They will be handling the vast amount of information of Government and society in this Nation. They accent our point which is, in Earth conditions we have quickly to translate this kind of speed of information, organization, and communication, down to about 40 or 50 bits per second for human use.

The next is simply an example of how one of these light beams is capable of such generation.

In doing so, it loses very much of its power, so we have oncoming a worldwide system of photonics which will enable radio handling beyond the radio system we use now.

By showing the progress in calendar years, we moved along fairly smoothly for several years, until the advent of photonics, which has jumped up the efficiency so much that we know that we will face a society much more supported by communications and information than ever before. But this will exacerbate the problem of getting these enormous information volumes down to this 40 or 50 bits a second in an emergency where we have to have decisions.

The next is simply a reminder that light waves do, however, function in the same way that radio waves and telephone signals over your line do. That is particularly so when you use digital and coding systems.

There are many exciting alternatives offered by the new speeds and efficiencies of electronics and photonics.

The cellular plan which has not been decided on but which is terribly important for emergencies is important, because you could have portable telephones throughout the Nation interconnected through the network we showed earlier but operating independently. The walkie-talkies are a rough approximation to it, but do not interconnect and provide a system as provided by this cellular system.

These things are all possible as you have heard because of integrated circuits of high economy. Here is a microprocessor of major computer capability of a few years ago.

The processing power of those machines is moving expeditiously. Here are some with very high capabilities and therefore, we can build an emergency system on decentralized, highly independent processing of information and communication of it, if we learn how to translate the very large volumes these things will handle into a form useful for people which can be done.

The costs of doing that in these circuits is going down expeditiously. You see the reduction, how cost in dollars per circuit has gone from say, \$1, 20 years ago, to a very fraction of a mill or one-hundredth of one-thousandth of a cent in this present time as we are actually getting down this curve very well.

So here is a country in its very compelling missions of protecting people faced with a resource for doing information processing which is very economical, and we must learn how to work that in. Some of your subsequent witnesses, Mr. Chairman, will have very cogent comments on that. Mr. Lewis, Mr. Hicken [phonetic] others are aware what can be done.

The whole application of these schemes is not limited to the emergency knowledge of a particular event or of a disaster or hostility, but is being extended to our general knowledge capabilities; Colonel Hanes [phonetic] who is here this morning has been active in developing a national network. Here is one we are doing linking the major research industries of the company.

This provides a base for knowledge of normalcy—it provides a population of people who can react to the information needs of emergencies in ways which have never been envisioned or mobilized by any nation yet. This is real and should be taken into our planning.

The next is a reminder that extraordinary facilities are coming out of these digital and coding systems. The coding of photographs, such as the coding of earthquake areas, can be analyzed and tracked. This picture begins with a digital synthesis of President Lincoln's visage. These elements can be tracked through and managed in the small machines we mentioned, as well as somewhat larger machines. So if this were a hurricane area instead of the essence of a visage, one would be able to tell persistently what has changed, what kind of alterations there were, without having to reconstruct the whole image and in doing so, losing the human observer's ability to determine what has changed. Here, 40 bits per second limits the knowledge, but the machine can pick out what parts of that knowledge are important.

The ways this kind of capability can be created are expanding explosively. This is a machine to make the crystals that are the essence of the circuits and the sensors that we just talked about. This is a very high vacuum apparatus, perhaps 10 to 20 times better than several years ago, and the atom is used to create these crystals.

The next shows an electrograph of an atom to manage these digits we are talking about so that the optimal efficiencies will be obtained.

Here is where nature does some of this. Here is one of the crystals we were able to synthesize in our laboratories showing the compartmentalization in which, as best we can tell, nature handles communication, does a passing of knowledge of how the structure can go.

This is vastly more subtle than we have ever been able to do. These are both of molecular dimensions.

Next, beyond all the apparatus, however, and the devices lies the ingenuity of the person. Here is where your witnesses will have very interesting comments, Mr. Chairman, because the software technology, the programming of these systems is actually what is essential to making the transition between the sensing of the event, the emergency action, the bomb-dropping, or the hurricane, and the translation of that into a form which the planner, the administrator, the emergency corps can use the information and go into action. Here again, the country is lucky we are creating a new population of people skilled in this, and we believe the reprogramming of these machines will lead to new capabilities of making words intelligible and effective.

We would conclude from the programming of these machines such as in the whole range of new software, with the hardware that we have so quickly referred to, we will have a new way of making simple words come out. We will submit, and have already submitted, in working with the FEMA, methods for prose construction which is machine-human interchangeable.

That is my main report as to what science and technology can do. If that human machine interchangeability is done, we shall have enormous strength.

[The prepared statement of W. O. Baker follows:]

PREPARED STATEMENT OF W. O. BAKER

The theme of these hearings on emergency management is an historic recognition that the technical capabilities which have brought us into the Information Age can help to protect our people in natural and man-made disasters and other emergencies. Indeed there is special challenge in this situation now, because emergencies usually cause, socially, information crises, in which rumors have long stimulated mass action, such as panic. Organized responses to emergencies must be quickly designed on the basis of knowledge of events. These have to be, in turn, quickly and simply described and understood. Further there is a psycho-social element on such information handling. For emergencies and disasters commonly include information that people don't want to hear, about matters classically reacted to as "unbelievable."

These latter factors which are enormously significant in popular response to disasters and emergencies put a special load on new and sometimes fragile information science and engineering. That is, the human transfer step has to be done in the most simple, universal, and credible terms, usually with high redundancy and exceptional reliability. The now —

classic Orson Welles Martian broadcast, and the radio announcements of the attack on Pearl Harbor, both of which we experienced, are interesting reminders of the informational vulnerability evidently associated with the psychological impact of the medium and the nature of events.

Accordingly, in reporting to you on the role of information science and technology, we note a need for obviously the most extensive modern sensing and communications network. That has been recognized, although not fully implemented, for more than a decade. What is presently under the FEMA cognizance is particularly functional for weather severities, including hurricanes and tornadoes. It involves since 1964 an Emergency Broadcast System (EBS), first set up for the President to report any acts of war. This was as a result of our studies in the late 50's and early 60's on surprise attack, and the new speed and damage dimensions of intercontinental ballistic missiles (ICBM). However EBS can now be used for weather condition announcement, power failures, fire, hazardous material accidents, etc. Inputs for its management obviously involve the FCC, the National Weather Service, state and local emergency functions, and The National Industry Advisory Committee. There is also functional around the clock a National Warnings System (NAWAS) centered at the National Warning Center at Cheyenne Mountain, Colorado and linked with the National Weather Service to more

than 1270 warning points. Likewise some 3,000 communities are involved in various local emergency measure schemes for responding to weather and other natural or artificial damages.

Now the point in summarizing this network situation is that it alone would demand new and strong technology for communications, resistant to disruption on land, sea, satellite or derived means. That technology is moving along, with new capabilities such as rugged digital radio, light-guide cable system, and small roof top and portable satellite receiving stations augmenting the already unsurpassed continental common carrier, special purpose, and military networks that we have.

However, overlying all this is our earlier point about the crucial role of the human interface and the extraordinary sensing and organization of information which has to be reduced to simple and credible terms for decisions and actions at the end. Now here, modern information science and technology give us a very sobering message. It comes from the confirmed theme of communications/information theory. This says that all knowledge and signals can be put into digital form by encoding through simple zeros and ones or on and off electric pulses or light flashes separated by darkness, etc. For now knowing that all information can be

expressed this way, whether initially as words, pictures, numbers, diagrams, or whatever, we can begin to compare the speeds and reliabilities of various informing processes. By a series of behavioral-engineering experiments we have a few years ago in our laboratories pretty well established that the maximum information input and output of the human system is forty bits a second. There are, of course, considerable variations and some dependence on language and culture. But we have been surprised and interested to find that not much more than that can be counted on for a hearing rate, a speaking rate, a keypunching rate, a recognition rate or the like. Of course, people are exposed to millions of bits per second in a single television picture or a photograph or complex diagram and they do react very rapidly. But the indication is they abstract information, despite many cues, only at a rate of about forty bits a second.

Now this is entirely compatible with the conventional signaling processes of civilization for thousands of years, including even the great advances of the Nineteenth and Twentieth centuries in telegraphy, which is of course, a digital and coding and signal method itself. Therein, a hundred or a few hundred bits per second are familiar, while semaphores, flag signals, and other important encodings are usually very much slower. In the voice telecommunications

we usually deal with five or ten thousand cycles per second of acoustics frequencies which appropriately digital sampled may involve a sixteen kilobit or even a thirty-two or forty-eight kilobit encoding for all the nuances. But the sounds are taken in, when reconverted to analog speech sounds, at the familiar forty or fifty bit rate, aided by the familiar and essential redundancy of language

But the anomaly, the challenge comes in when modern electronics (and oncoming photonics), particularly as dealt with in digital machines like computers, communications multiplexing, etc. easily handle information at a million, a hundred million, a billion, and in prospect a thousand billion bits per second. Through this we have an increasingly easy capability of gathering, organizing, and through the national network, communicating vast amounts of information that may be statistics on earthquakes (with images electronically derived) of the conditions over wide range of country side or cities. Or they may be hurricane paths or nuclear fallout zones from an atomic or nuclear event. But the human implications of these bodies of knowledge and especially the decisions that our emergency management systems have to make for the benefit of the people must be done by individuals, interfacing with the computers and communications terminals, at about a forty bit per second range.

Thus we need to design and to develop stronger interfaces in both the national military command/control systems and the emergency management plan. These should begin at the highest levels where the most crucial decisions are made, in the White House and its derived agencies, and extend through the hierarchy of officials. We need to design and develop an optimal transition from the very large information domains of global satellite sensing, surveillance, continental sensing, and observation inputs and ongoing data bases like libraries, and academic networks. All must serve the individual user and decision maker.

Now this mission has, of course, many of the characteristics of modern management information systems, which are flourishing in a thousand forms around the world, but which do not yet take advantage of another part of modern science. That is the electronic and photonic circuitry which does the encoding, the processing, or computing, the management of transmission and switching, and thus of the circulation of crucial knowledge. This has all come since the mid-Century from our discovery of the transistor and of the associated families of solid state devices, electric and magnetic. These marvelous systems are supplemented also nowadays by sensors from solid state devices like the charge coupled-device, transducers, other imaging systems, heat and radiation sensors, and the like.

They are all embodied now in exceedingly thin film subsystems called integrated circuits, which can manage the processing and communication in the ways we have described. The capacities and costs have gone in complementary fashion toward efficiency unexcelled in the annals of technology. Particularly, however, in terms of information systems, small units of these innovated circuits can comprise microprocessors and microcomputers which can be spread about the nation (we estimate there will soon be more microcomputers in the U.S. than there are total people. This is not an idle irrelevancy but a recognition that really significant augmentation of logic and memory and knowledge organization is being embedded in our society.)

So what we are saying about emergency management is that we should start setting up nationwide systems, beginning in Washington, where little machines to record, arrange, check and communicate information are used on a scale of hundreds and thousands and eventually orders of magnitude beyond that. But they must be arranged so that they come down to action in the nation's brain. Any old organism, but most particularly people, have a neuron network of complexity and extent exceeding anything we are yet proposing. The structure of that has given us indeed ideas about how to arrange this national nervous system that we are proposing.

In the doings of this analog to a nervous system, the crucial unit will still be words. That, too, is curious, since as we have said the elements that are handled, processed and communicated so quickly are encoded in electromagnetic forms. And they are digits, frequently or sometimes parts of electromagnetic waves. Yet in the end we have to operate the network with words, and they are subject not only to the slow perception and expression channel of about forty bits a second, but they are also full of ambiguities and uncertainties. Accordingly, we should use science and technology to sharpen and enhance the meanings of these words. We are really only at an early stage of the machine dissection, and reconstitution of natural language, in order to know its morphology. This is going to be a rapidly moving frontier of great significance for crisis management and other administration. Nevertheless, a good start is in hand, and it includes such growing operations as what in our Laboratories is called "the Writers Work Bench". This is a system of prose organization, and specification supported by the UNIXTM computer system.

These resources do many different things that we do not have time to recount now, but essentially they simplify and expedite finding out what happens to key words and action sentences like "send a truck", or "get a doctor" through a whole range of files and reports and summaries and

confirmations. They permit the rapid and precise combining of descriptions of a situation like a hurricane path or a hostile event. They then, currently provide a discipline through the computer processing of the text so that tight, uniform and consistent formats come out. We believe and are advocating for command and control practices currently, that working these computer-shaped text statements through the information gathering, coordinating, and decision-making process will lead to new speed and validity of action.

Certain rudimentary tests of this have already worked out. Thus, industry uses specifically formatted voice instructions for assembly line and work bench manufacturer especially in complex circuits and device assembly work for communication equipment, computers, control machinery, and the like. We have observed in our own Western Electric factories that computer generated voice, rather than that pasted together from human-voiced instructional tapes, leads to care and precision of statement. Indeed, it even has a certain consistency of inflection and tone, which are favored by the people reacting to the instructions. We believe that such automated voice output, and slow teletype output command systems in both military and civil crises management will greatly improve the way information is used.

We know that by this route some further adjustment between the multi-^{micro}bits speed of processing of knowledge and the forty bit intake and output by people can be achieved.

BEST COPY AVAILABLE

We urge that exercises and procedures gradually embodying these capabilities be undertaken.

We have not explored in this brief overview the huge and proven role of information and communications science and engineering in handling data bases, printed records, and imagery especially as obtained in high altitudes. Nevertheless we can be assured that these applications of modern digital photonic circuitry and display are available. We also have said little about the vulnerability of these systems to network disruption and damage by nature or weaponry or sabotage. On the latter, however, we have emphasized the decentralization and disruption of microprocessors and small inexpensive digital units because this is one of the best ways we think of assuring reliability. However, it should be pointed out that almost every hardware element we have mentioned nowadays depends on the functioning of a junction device, which is a p-n junction in a crystal and these can be severely sensitive to radiation damage.

Mr. GORE. Thank you very much.

That was fascinating. I wish you could just take off a little time and do this for us. I think you probably understand the potential and practical aspects of it better than anyone I know.

Could you comment on the course of development over the years of emergency management systems for dealing with information? This may be an unfair question, but what I have in mind is an analog to that graph you showed demonstrating the steady increase in the capacity of information systems, in the generic sense, over time. You talked about how optic systems are now changing that curve dramatically.

Is it possible to convey some understanding about what similar developments have been with respect to emergency management systems?

Mr. BAKER. Yes, sir, the curve would lie not just 20 or 30 percent or 50 percent below the percent showed, but orders of magnitude below it.

The system started by digital smoke signals, then moved to flags and semaphores.

Mr. GORE. And digital lanterns, one if by land, two if by sea.

Mr. BAKER. That is right. Dependence on those systems was so strong, they worked, and dependence on some of the newer ones was so little because lots of them did not work, that the great traditions of command and control kept with the flags, the semaphores, and telegraphy. Telegraphy is still orders of magnitude below what we are talking about, maybe 100 bits a second, but lots of it is less than that. Those are the things that have characterized emergency management during most of its history.

The translation that we spoke of to words which are precise and simple and dependable is still very much in its early stages, and we believe that it ought to be accomplished by some retention of things like telegraphy. The prose you get out of telegraphy, which is still a major part of the teletype system, we believe the prose you get out of that, which is simple, because there is no capacity to do anything else, ought to be retained and worked through the high digital machine, so you get a smooth transition to the improvement you are applying.

Mr. GORE. If you put this into a concrete example of what could be in place in the future, what would that example look like to you?

Mr. BAKER. It would look like a diagram of Three Mile Island, where the radiation levels, the wind conditions, the transport, the concentration of people, and the rest of the environ, were displayed in compartmented precise form so that simultaneously that information was available to the Administrator, the planner, ultimately the President, and this incredible confusion and word disruption of reality would not take place.

The words would have to come out eventually, but they would come out of the digitally synthesized environ of the event. There is just no reason, as we pointed out in connection with our photographic image example, there is no reason why that cannot be constructed.

Mr. GORE. In your example, would FEMA supply that information to the NRC, or how would that operate?

Mr. BAKER. FEMA should be the focal agency for all such events. Therefore they would receive and synthesize this complete information. We have the capability of sensors; any nuclear plant ought to have these around so they will know what is happening. FEMA then by the aid of some of the machines and software we are talking about could quickly transform that to the human usable form which the President might want, which the military might need, which the civil defense authorities would immediately benefit from.

Mr. GORE. Now that would require compatibility between the sources of that information and FEMA's ability to receive it and synthesize it, is that correct?

Mr. BAKER. Indeed that is so, and that is where the country again is fortunate, because our communications and information handling systems are sufficiently compatible, are sufficiently interconnected so that such a format could be achieved.

Mr. GORE. If we set out to achieve it, what are the major problems you would expect to first encounter?

Mr. BAKER. One thing is that we would have to get away from the current support of fragmenting all of our resources, fragmenting communications, fragmenting our responsibilities for information handling and sensing.

Second, we would need to encourage industrial cooperation and interaction in coding systems and the whole software program so they would fit together. Again, the thing that can be managed from Washington, but in the face of efforts to fragment our resources, will not work.

Mr. GORE. What do you mean by fragmentation?

Mr. BAKER. Well, both the antitrust pulses and many rulings prohibit the exchange of information on how to handle and communicate, and also the content of it among industries.

Environmental measurements, for example, that can come from factory emissions, vehicles, or other things and which, as we know, occasionally constitute emergency conditions are not freely exchanged among industries, among components of our society.

Mr. GORE. What kind of problems would you anticipate related to training of key persons to operate advanced systems of the kind you are discussing?

Mr. BAKER. That requires very good experience in digital programming and machine operation, computer engineers and technologists which are highly needed in our industry nowadays, anyway, and which the Nation has a very severe shortage of. Your parent committee, Mr. Chairman, has been extremely interested and sympathetic in hearing our great concerns about the education and the scientific and engineering training of this community of people. They are indispensable, they are invaluable, and we have very few of them.

You will hear some of those problems from Mr. Hicken [phonetic] and others during these sessions. We just have no chance of getting those people. You again are identifying a crucial thing unless we increase our output.

Mr. GORE. Can you identify the major data bases that you think should form the nucleus of a beginning on this path?

Mr. BAKER. We have some very powerful ones. The satellite imaging and the geodesic and Army and other map services have been combined so there is a very fine data base for the geography, and to some extent, the demography of the Nation. We believe there are increasingly important data bases on the atmosphere building up in the NOAA and other agencies. The FEMA is indispensable in pulling these together. The ones I mention are some of the largest and most interesting collections of data about the state of our Nation that is imaginable. The same is true of the National Health Service. They know of the normalcies of illness, but they are not coordinated. These data bases are so huge that up to now people thought well, you cannot interact with them anyway. But we are reporting to you with modern machines and communications you can. Therefore, the circumstance is that someone has to pull them together, which FEMA is chartered to do but it has not yet been possible to do it.

Mr. GORE. You mentioned four, the geodesic or geographic covering the land mass of the United States; the demographic and population data from the Census Bureau; the atmospheric data from the National Weather Service; and epidemiological baseline data from the Public Health Service, and I suppose the Center for Disease Control and other components of that service.

Any other major data base?

Mr. BAKER. In terms of transport and supplies, there are increasing data bases. We believe that both the agriculture area and some of the transportation folks would know what food and some other supply distributions are in a general way. We doubt if those data bases have been pulled together with sufficient scope to be satisfied. But they are under way.

Mr. GORE. The model you have in mind, then, is a digital capability that would be focused at FEMA with the ability to access all of those data bases and others and select very quickly the information directly relevant to unfolding matters of immediate concern and then provide that information to the decisionmakers who are attempting to cope with the matter at hand?

Mr. BAKER. Yes, sir, you have articulated very accurately our model for those resources. Now, one adds to that, as you earlier implied, a similar model for sensing what is needed, what is actually going on out there, which may be a hurricane, an earthquake, or a geographic one, it may be a disease measure, or in the case of a nuclear event, the radiation levels, et cetera, those can be brought together.

Mr. GORE. I suppose we could add a third thing—what comes to mind is a file on key human resources, experts, scientists, and the like, who have the ability to assist quickly in analyzing developing emergencies. Would you include that also?

Mr. BAKER. Yes, sir, we feel that would be important. There are some small exercises in the medical and health field and there are some in materials management and engineering that are going that way. Indeed, I think that would be very valuable.

Mr. GORE. In going back to the Three Mile Island model, that last file would have been quite helpful in the early hours of the Three Mile Island incident. I suppose the demographic atmospheric models would have also been of enormous help in that example.

Mr. BAKER. I think it would have prevented the agony the people went through, because it turned out the actual measured levels were not what were assumed at all.

Mr. GORE. Well, you have gotten us off to a good start. I certainly appreciate the amount of work that you obviously went through to give us the framework within which to explore this enormous potential and the applications which we could engineer for that potential, and thank you for once again playing such a constructive role.

Mr. BAKER. Thank you, sir.

Mr. GORE. I would like to call next Maj. Gen. Bennett Lewis, Executive Deputy Director of the Federal Emergency Management Agency.

Thank you for coming, General Lewis. We are delighted to have you and we invite you to proceed with your testimony.

STATEMENT OF MAJ. GEN. BENNETT L. LEWIS, EXECUTIVE DEPUTY DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY, ACCOMPANIED BY DR. CHARLES M. GIRARD, ASSOCIATE DIRECTOR (DESIGNATE), RESOURCE MANAGEMENT AND ADMINISTRATION, AND BRUCE J. CAMPBELL, ASSISTANT ASSOCIATE DIRECTOR FOR INFORMATION RESOURCES MANAGEMENT, RESOURCE MANAGEMENT AND ADMINISTRATION DIRECTORATE

General LEWIS. Thank you, Mr. Chairman, and members of the subcommittee.

I am pleased to follow Dr. Baker, who is on the advisory board to General Giuffrida, the Director of the Federal Emergency Agency. Later on, I will reference an area where he has been giving us some help.

I know there may be some redundancy in my remarks and those in Dr. Beal's statement, but I would like to read from a part of his statement. It is written very well. In it he said:

The President has instructed the Federal Emergency Management Agency (FEMA), under the direction of General Louis Giuffrida, to make special efforts to ensure that this Administration is properly planning for the entire range of hazards that confront us. And, the Administration fully supports General Giuffrida in his application of science and technology to the policies, programs and priorities of that Agency. FEMA will have direct access to the White House for current and short-range emergency management planning and operations as well as for the medium and long-range planning necessary to ensure that the White House is able to immediately respond to future potential major emergencies.

I think that contains the key to FEMA's success in this area, that is, access to the White House and support from the White House.

I appreciate the opportunity to speak to you today about the capabilities and plans of FEMA in the area of information technology as it is applied to emergency management. My remarks at this hearing will address the missions and roles of FEMA and the general form of our involvement in information technology. The Agency is prepared to return at your pleasure to review in greater detail the specific information systems and technologies FEMA has developed, is using, or plans to pursue.

As many of you are aware, FEMA prepares for and responds to peacetime emergencies that are caused by nature or are man-made

and with wartime emergencies. Our concern is with the effect of these emergencies on Government's operations, on the civilian population, and on the civilian economy's ability to meet national security needs. Natural emergencies include, for example, floods, fires, earthquakes, and severe weather. Examples of manmade emergencies include the consequences of terrorist acts, arson, civil disturbances, major interruptions in the supply of natural resources, and spills of hazardous materials. War-related emergencies involve civil defense, continuity of Government, and the ability of industry to meet both military and essential needs of civilians. In the cases of potential emergencies, the major activity areas are preparedness, mitigation, and where possible prevention. In the cases of actual emergencies, the major activity areas are response, recovery, and in some cases compensation.

In addressing these emergencies, FEMA coordinates the efforts of other Federal agencies and works with State and local governments and volunteer agencies. The major volunteer agency is the American Red Cross, and I know you will be hearing from Mr. Vessey a little later. We work together. Successful coordination of the actions of all these parties requires access to accurate, appropriate, timely information, and excellent communications. In the immediate aftermath of a major emergency, large quantities of information must be assembled from disparate sources, quickly processed and analyzed, and translated into a form useful for decisionmaking at many levels up to and including the President of the United States. Before major emergencies occur, FEMA is involved with large-scale management of a different kind of information—studies, analyses, and plans that support preparedness programs to mitigate and prevent emergencies and allocate resources. We at FEMA are managers, users, and providers of information in a very large way. We have a great interest in the topics being addressed by this committee.

FEMA was created by Presidential Reorganization Plan No. 3 of 1978 and Executive Orders 12127 and 12148 in 1979. At its start FEMA was a loose amalgamation of five agencies with functional activities all directed at particular types of emergencies. FEMA's new organizational structure is designed to take greater advantage of the functional similarities among its various preparedness and response activities and to permit greater use of modern information technology, such as distributed computer data processing and telecommunications system networking. With these changes, we will be able to coordinate our work better and serve our clients more effectively and efficiently.

I would now like to take time to talk about our new organizational structure, because we feel this will provide better service.

The first I will describe is the State and Local Programs and Support Directorate. The directorate is the focal point in FEMA for all Federal emergency management programs which impact on State and local governments—this would include technology transfer—in planning, preparedness and mitigation, crisis management, and emergency response and recovery efforts. Its programs provide for both technical and financial assistance to State and local governments.

This directorate operates the Emergency Information and Coordination Center, the focus for centralized collection and management of disaster and emergency information in FEMA. This was discussed very well in your dialogue with Dr. Baker. The flow of information—accurate and timely—is critical to FEMA's coordination and management role in emergency situations.

This directorate also administers the Disaster Relief Act. When disaster strikes, under this act the primary responsibility for relief and recovery activities belong to the affected local governments and the State. When a Governor determines that the disaster is beyond their capabilities, he may request Federal supplemental assistance under a Presidential declaration of a major disaster or emergency. In that event, FEMA regional offices, augmented by other Federal agencies, make joint surveys with the State to assess damages and requirements for assistance. Damage and impact information is collected at the local and State level, evaluated by FEMA program managers, and a summary report and recommendation is made to the White House through the Director of FEMA.

When the President declares a major disaster, FEMA establishes a disaster field office and disaster assistance centers in the affected areas. The Agency administers programs that provide relief and recovery assistance to the disaster-stricken communities and to disaster victims and coordinates the total Federal response. FEMA also coordinates the voluntary disaster relief organizations in responding to major disaster situations.

Disaster mitigation activities are performed to help insure the future safety of life and property, disaster relief and flood insurance activities of our agency are coordinated in order that communities and individuals might be prepared for the most commonplace disaster—floods. All of this requires communication and information flow—to disaster victims, public officials, program managers, Federal agencies, the Congress, and the White House.

State and Local Programs and Support also is responsible for plans and programs related to technological as well as natural hazards arising in wartime and peacetime emergencies. It develops national contingency plans which prescribe Federal efforts to cope with technological hazards such as radiological or hazardous materials incidents, and provides technical or financial assistance to State and local governments to eliminate or lessen the potential effects of such hazards. It also develops and administers civil defense programs and support systems to assist State and local governments in maximizing the survival of the population and resources through effective crisis management planning and the development of improved response capabilities.

These activities depend upon the operation of a reliable, survivable emergency communication system. To maintain such a system, FEMA provides technical and financial assistance to State and local governments for the upgrading of their emergency communications and warning systems. You will be hearing later from General Ott. He will be describing a facility in Arizona in which FEMA participated. These systems assure the rapid dissemination of warning to governments and alert notification to the public. I have not brought any pictures of hardware, but there are two prototypes indicated by Dr. Baker. We used one he showed you and were able

to establish very effective communication for people on-site. This exercise took place in Nevada, and we were simulating the State of California. In this exercise we worked with the State and local people.

The second directorate of FEMA which I will describe is national preparedness programs (NPP). This directorate develops national policies, plans, and requirements for operational programs to meet future and long-term civil emergency preparedness and planning needs. NPP's activities are closely integrated with other elements of FEMA, particularly with the operational activities undertaken by the State and Local Programs and Support Directorate.

The programs of the national preparedness programs directorate are administered through three preparedness offices—resources, civil, and government. This Office of Resources Preparedness identifies, evaluates, and prepares for current and possible future shortages of natural, industrial, or economic resources which could have disastrous effects on our economy and our national security posture. This Office develops proposed methods for the mitigation of such threats through stockpiling and/or through encouraging the development of additional domestic capacity. This Office also makes assessments of the Nation's ability to mobilize in time of war or other national emergencies and develops concepts, plans, and systems for economic mobilization in a range of national and civil emergencies. This office develops and uses complex modeling techniques for the economy which involve extensive use of computer technologies.

The Office of Government Preparedness develops policies, plans, and requirements for Federal programs to insure survival of the Presidency and continuity and effective operation of Federal, State, and local government during national emergencies. This office guides and coordinates the plans and programs of other Federal agencies in this area and insures that Federal plans and systems, legislative authorities, and delegations of authority are adequate to respond to the full spectrum of possible national emergencies. This office relies heavily upon emergency warning and notification, situation assessment, decisionmaking, and the transmittal of directions for response. All of these functions rely heavily on information and communications technology.

The Office of Civil Preparedness develops the long-range plans and programs which are necessary to maintain an effective national capacity to protect the population of the United States and key governmental and industrial components against enemy attack, to mitigate natural and technological hazards, and to minimize the negative consequences resulting from domestic disturbances and terrorism. Much of the strategic planning work in this area is heavily dependent upon the availability of timely data and scientific and technological information which can be employed in the development of improved policies and procedures for applications across the comprehensive emergency management spectrum—mitigation, preparedness, response and recovery.

An example of close cooperation that I have described between NPP and the State and local programs and support directorate (SLPS) can be found in the civil defense program. In this area, NPP is responsible for developing a long-range strategic plan for

the program which is based upon assessments of the threat, research findings, assessments of potential new and more effective approaches to the protection of the civilian lives and property, and surveillance and analysis of changing conditions, with SLPS being responsible for translating the strategic plans into operational capability. In this area they work hand-in-hand with FEMA regional offices, State and local governments, and the private sector in such matters as the support of emergency management staff and facilities, emergency management planning, emergency communications for warning, and situation management and response actions designed to minimize injury, death, and suffering among the population, as well as minimizing damage to, and loss of property, and economic dislocation. We also have within our organization the Fire Administration, whose goal is to reduce by 50 percent the Nation's loss of life from fire by the year 2000. The Fire Administration also seeks significant reductions in property loss and injury from fire. The annual death toll from fire exceeds that from all other natural disasters combined, but deaths from fire occur primarily in ones and twos, not in the large numbers and major incidents that are the norm for other disasters. In recognition of the diffused nature of the fire problem, the Fire Administration works to improve the levels of fire protection and the cost-effectiveness of public fire services in the United States. We do this through three offices.

The Office of Fire Protection Management has the lead in passing on usable programs and techniques to State and local governments. It maintains resource networks and program exchange systems to do this.

The Office of Fire Protection Engineering and Technology promotes the development and stimulates the use of fire-related technological developments, such as automatic fire detection and suppression devices; works to improve fire safety in structures through improved code enforcement practices; develops and promotes equipment and techniques to improve firefighter safety and health; and assists other Federal agencies and private firms and associations in obtaining and interpreting data on fire protection issues.

The third office is the National Fire Data Center, which develops and disseminates statistical information on national fire trends and patterns, and assists States and localities in developing information useful in solving fire problems. National statistics compiled from the National Fire Incident Reporting System are used to prioritize fire problems and programs; respond to inquiries from State and local governments, the press and the public, and provide information on the likely impact of proposed Federal legislation.

The Federal Insurance Administration is a fourth major element of FEMA. It administers three federally mandated Federal insurance programs; that is, the National Flood Insurance Program, which currently insures about 2 million property owners against flood loss, the Federal crime insurance program, and the riot reinsurance program. To qualify for Federal flood insurance, local and State governments adopt ordinances to mitigate future flood losses. These ordinances are based on flood hazard identification maps and other technical data supplied to the communities through FEMA's directorate for State and Local Programs and Support.

The fifth FEMA directorate is training and education programs. We have established the National Emergency Training Center at Emmitsburg, Md., which develops and administers training programs in support of emergency programs at all levels. Resident programs will be coordinated with nonresident courses offered through the regional offices to support State and local training needs.

Finally, the sixth FEMA directorate is titled the Resource Management and Administration Directorate. It provides essential support services for all FEMA elements. Within this directorate, the normal functions such as personnel administration, comptroller activities, and general administration and property management support are carried out. The responsibility for insuring that a protected facility which provides Federal civil government heads the capability to respond even during serious emergencies is also managed by this directorate. This includes coordination of resources and economic dependence upon information systems, ADP, and telecommunication to insure stabilization throughout the entire spectrum of emergencies.

As you can see from the various and diverse FEMA mission responsibilities, all emergency related, the communication, ADP, and information processing capabilities of the agencies are central to program success. In mid-June of this year, 1 month after General Giuffrida was confirmed, we commenced a priority review of where we stood in this area, and established an information resource management team to: (1) Inventory our current requirements and resources for telecommunications, ADP and information management; (2) develop the fiscal year 1983 telecommunications and ADP budget estimates and issues for the Director; (3) develop an IRM information resources management organizational structure and management concept; and (4) develop the FEMA information management plan required by Public Law 96-511, the Paperwork Reduction Act of 1980, for OMB.

This study led to the establishment of an Information Resources Management (IRM) Office in August. This office is part of the Resource Management and Administration Directorate. It provides policy, direction, guidance, and goals for the planning, management, and budgeting for information resources in support of FEMA, to include areas such as our Emergency Broadcast System (EBS) oversight responsibilities.

This office is also responsible for the day-to-day management of the FEMA ADP and information management systems plus our extensive telecommunications and warning systems. For example, it manages the Civil Defense National Teletype System Network, the CD National Voice System Network, the CD National Radio System, the National Warning System, the Washington, D.C., Warning System, and our classified systems.

While we are proud of the progress we have made in this area, we plan to accelerate this effort. Within this area of information resources management, we have established seven overall goals. First, to develop and begin implementation of the FEMA National Emergency Management System. Second, to develop a 5-year plan containing short-, mid-, and long-range information resource goals. Third, to improve FEMA modeling techniques and requirements.

Fourth, to improve the survivability and quality of communications and information needed by decisionmakers in a nuclear emergency. Fifth, to improve the warning, communication, and public information systems available. Sixth, to coordinate FEMA data requirements, establish quality standards, and develop improved data handling techniques. And seventh, to develop the data base, information processing capabilities, and information displays needed to support the Emergency Information Coordination Center. All of this, of course, will take advantage of what is developed here and of the talent, skills, and experience available from our advisory board and other Federal agencies.

The establishment of a centralized Information Resources Management Office promotes multiple use of information resources, standardizes information equipment across all programs, and reduces the costs through combined purchasing. This office will provide FEMA with the ability to provide a central point of contact within the Executive Branch responsive to the information needs of emergency managers at all levels of government. It also allows us to implement the provisions of the Paperwork Reduction Act in the manner Congress intended.

In the past, we found that FEMA did not necessarily get the cooperation required from other agencies. This situation has changed. I can report to you some examples.

Last week I escorted Secretary Block to the FEMA special facility. In the recent past, Secretary Regan, and Secretaries of other departments and agencies have been taken on visits. I have been meeting with Assistant Secretaries who are responsible for emergency management. A substantial effort is underway to take near-term actions to improve this country's ability to respond to wartime and peacetime emergencies. It is recognized that civil preparedness is equally as important as military preparedness. The direction from the White House in this regard is very clear, easy to follow, and will be followed.

The Federal Emergency Management Agency is committed to develop information systems to support both our peacetime and wartime responsibilities. We intend to commit all resources necessary to insure that we develop emergency management systems required to help minimize loss of human life and property by the American people.

Mr. GORE. Thank you very much. That was very impressive testimony.

Let me ask you some questions about the Information Resources Management Office, IRMO. Is that acronym becoming familiar within the Agency?

General LEWIS. Yes. Bruce J. Campbell and his boss, Chuck Girard, are here. I wonder if I could have them come forward. Bruce Campbell, formerly with the National Communications System is now with us.

Mr. GORE. For the benefit of the reporter, Charles Girard is seated in the center, and Bruce Campbell to the Chair's left.

Mr. Girard, what is your position?

Mr. GIRARD. When confirmed by the Senate, I will serve as the Associate Director for Resource Management and Administration for FEMA.

Mr. GORE. Bruce Campbell, what is your position?

Mr. CAMPBELL. Assistant Associate Director for Information Resources Management.

Mr. GIRARD. In addition to providing information resources to the Agency, other support including manpower planning, the comptroller function, which encompasses the budget process, an accounting process, and acquisition management is handled by the Directorate, along with the responsibility for security and administrative support.

Mr. GORE. Thank you.

Mr. Campbell, you are head of the Centralized Information Resources Management Office. What do you call it for short?

Mr. CAMPBELL. IRM.

Mr. GORE. IRM. How many people do you have working for you in IRM?

Mr. CAMPBELL. Right now, roughly 340 to 350 people. We are in the process of restructuring the entire organization to bring into a telecommunications management office and a computer management office.

Mr. GORE. Would you move the microphone a little closer?

Mr. CAMPBELL. That includes all our Watch Center people and all the people in our sites and at the various computer centers we have.

The office was just established August 27. We have a goal of 30 days, which will be up tomorrow, to formally realine and reassign all the people into that new organization.

Mr. GORE. Now of the 300 to 350 people in your office, is it fair to assume that most of them are at work with on-line responsibilities in the Teletype System Network and the National Voice System, the CD National Radio System, the Warning System, and the D.C. Area Warning System and the Classified Systems.

Mr. CAMPBELL. Yes, sir, for the telecommunications management side.

Mr. GORE. Those are all included among the 300 to 350?

Mr. CAMPBELL. Yes, sir.

Mr. GORE. How many people are at work developing this new plan?

Mr. CAMPBELL. All 350 of them.

Mr. GORE. Seriously?

Mr. GIRARD. Mr. Chairman, if I might add, when Bruce says all 350 of them, he is not being flip. One of the problems we had had in taking on this mission was, in fact, that some of the people who had been involved in the past in the ADP and telecommunications functions in the Agency were unknown to the Agency itself. So Bruce has gone to the lowest level of individual in the organization to determine what is being done. With General Giuffrida we learned that many of these people did not even have job descriptions prepared, so essentially, they are all involved in the realignment function within FEMA.

Mr. GORE. All of these systems—the teletype, the National Voice System, and the others—are in the range of that 40-bits-per-second that Dr. Baker referred to, are they not?

Mr. CAMPBELL. The voice system and the radio system; yes, sir. The teletype system is not as high as what Dr. Baker says is theoretically possible.

Mr. GORE. It is not theoretically possible; it is actually possible.

If you and I went down to Radio Shack with some money and the cooperation——

General LEWIS. That is the key.

Mr. GORE. I understand. We could get an off-the-shelf system that would be a lot better than what we have now, and the savings when the emergency occurred would probably dwarf the investment made. Would you agree with that?

Mr. CAMPBELL. I would agree wholeheartedly, and that is part of the problem, the fact we have to spend money to save money, and that is the modernization of existing systems.

Mr. GORE. You need some supply-side emergency management here, I guess.

What was your reaction, General Lewis, to the interchange Dr. Baker and I had as to the model of accessing the digitized information bases now readily available?

General LEWIS. My first reaction was that I was very pleased it was taking place. Dr. Baker and I had a similar discussion earlier as we brought him and others in to discuss the Information and Coordination Center we are planning. We have one at the present time, but we are going to improve it, and we are seeking his help.

We already have, by the way, programs where we are pulling data together. I alluded to some fairly primitive ones where we go out on the site and make joint surveys with other agencies and the State. This is basically an action that involves assembling the information to assist us in making decisions as to the Federal help that should be provided.

But in the area of planning, perhaps the radioactive fallout from a nuclear accident, either from a weapon, or should there be one, at a power station. There are systems now being worked on. For instance, at the Oak Ridge National Laboratory where they are pulling together weather data and creating fallout patterns. We have been able to do that for years, but we certainly are not satisfied with where we are. We propose to move forward and gather all data that is essential.

Back to the point, I am pleased the discussion is taking place. We are all a part of this activity, the executive agencies of the Federal Government, the White House, and the Congress. We would like to be able to make a trip to a Radio Shack—we are not advocating patronizing any specific commercial firm—to modernize our system and to provide hardware that will permit access to the existing data bases.

Mr. GORE. We often ignore efficiencies of specially designed hardware and I wonder if you have any thoughts on how the State and the local authorities might begin planning to coordinate, in the future, hardware compatibility with FEMA, in order to access the data which you will be capable of providing them.

General LEWIS. I can give you a specific example that involves FEMA and the State of Arizona. You will be hearing from General Ott and you may want to ask more of him. On the Federal side, we are concerned about and working on the problem of compatibility.

Mr. GORE. We will be hearing from him tomorrow.

General LEWIS. We are trying to upgrade statewide and areawide communication capabilities. Arizona's system is a mobile communication unit that uses satellites. We are concerned about the link from Arizona's system into the Federal system.

I am not sure that is responsive to your question.

Mr. GORE. Well, partly. It might make sense, Mr. Campbell, as you look at the potential for providing data at a billion bits per second rather than 40,000 or 30,000, to make any transmission capability immediately compatible with readily available small computer units that States and local governments will eventually find cost-efficient for a variety of purposes, and which could be adapted to handling the information that you hopefully will be able to provide them in the future.

Mr. GIRARD. Mr. Chairman, if I might respond before we turn it over to the high-tech people. One of the things General Giuffrida and General Lewis have attempted—one of the first steps Lee Thomas, the associate director designate for State and local programs within FEMA, and I took was to insure, this prior to funding hardware for ADP at the State and local level, which would support information systems, and that we had the capability to review those systems through our IRM office. That is not to say we are developing standards, but rather a thorough understanding of what the State systems are.

Mr. GORE. Who provides the money for State and local governments to get this system? Is that LEAA?

General LEWIS. No, the Federal Emergency Management Agency.

Mr. GORE. Pardon my lack of information on this subject, but what is your budget on that line item this year?

General LEWIS. I do not have that number readily available.

Mr. GORE. Do you have a ball park estimate?

General LEWIS. I believe for emergency operation centers, something on the order of \$6 million. These projects are cost shared. This is not a total Federal grant.

We also have funds we provide for hardening commercial broadcasting stations to satisfy our warning systems. That is financed entirely by the Federal Government.

Mr. GORE. Against EMP?

General LEWIS. Yes.

Mr. GORE. Do you have an approved list of hardware and software from which applicants for these funds must choose?

Mr. GIRARD. Sir, when I alluded to the fact that we have not attempted to, nor do we have standards, FEMA does not have an approved list, at this time.

Mr. GORE. If you come up with a 5-year plan, say, to make possible the sharing of these vast quantities of data on a timely basis, that plan ought to include careful attention to compatibility between FEMA and the State and local authorities, and a necessary component of that goal would be guiding the purchase of

hardware and software that can be easily made compatible. Does that not make sense?

Mr. GIRARD. Very much so. That is why I deferred the high-tech answer to Bruce. Also, that is one of the reasons we were concerned, along with General Giuffrida and General Lewis, that there was not a capability base line. As a result, many of the grants which were given simply returned dollars to the States. The States oftentimes asked for guidance in these matters which FEMA at that time was unable to provide.

Mr. GORE. General Lewis, one of the lessons of Three Mile Island, it seems to me, was that FEMA looked great on paper, but when "push came to shove," the other Federal agencies did not really take FEMA seriously,

What can you do to make sure that they do take you seriously, and particularly in this area?

General LEWIS. I would think the actions we can do have already been taken. We have met with the heads of the agencies involved to insure an understanding of our respective roles and responsibilities. We have had either three or four meetings with the Chairman of the Nuclear Regulatory Commission and his staff, and we have met with other agency heads to include the Department of Defense, to assure they take FEMA's role seriously. I am satisfied that these meetings have already led to the result that you desire.

That is not to say that we do not have to follow up on these meetings to make sure we stay on track. There is designated a FEMA official who is responsible for coordinating other Federal agencies in the event of an emergency.

Recently, there was a test nuclear exercise. General Giuffrida and I attended, and by our attendance and participation we intended to demonstrate the role FEMA plays. Many are aware that the word "coordination" means cooperation. There is an awareness among Federal agency heads that their efforts must be coordinated.

Mr. GORE. Have you run any tests on the civilian side with tornadoes, nuclear plant disasters or the like?

General LEWIS. We have run some recently with the NRC and other Federal agencies on powerplants.

Mr. GORE. In that test, was any thought given to accessing the data bases from the National Weather Service, from the Census Bureau, from the geodetic data bases and the others Dr. Baker referred to, or is that off in the future?

General LEWIS. I am not aware of all the details on the specific exercise I have in mind. FEMA being responsible for offsite emergency preparedness, must be sure we can plot radiation patterns. This requires us to take account of radiation levels and wind pattern.

Mr. GORE. What about the other data.

General LEWIS. Again, I am not able to address it on this specific exercise. In the nuclear weapons exercise, we did rely on the Department of Agriculture, Health and Human Services to provide us their data bases.

Mr. GORE. Mr. Campbell, in the future, are you looking at this possibility?

Mr. CAMPBELL. Yes, sir, we have been in the process during the past 2 weeks of reviewing all the existing data files that the Federal Emergency Management Agency has on the various computer systems. One of the objectives is to come up with, at the direction of General Lewis, a composite list of the critical emergency management files that should be available to the decisionmakers instantaneously, population done by region, State, county, by political subdivisions, being one of the prime requirements. Our main problem right now is seeing what data we have in the file to support that and then what is its validity to if it is 1977 census data we have to update that.

The other critical files mentioned by Dr. Baker are also on that list.

Mr. GORE. Does that list just stay in the file? What are you going to do with that list?

Mr. CAMPBELL. That will be at the top of our project list for reviewing, validating, updating, and making it available to the crisis managers on a day-to-day basis.

Mr. GORE. I would like to now recognize my colleague, Mr. Brown.

Mr. BROWN. While I am taking up some time, Mr. Gore, you can be thinking up additional excellent questions.

Mr. GORE. I already have some, thank you.

Mr. BROWN. I am sure you gentlemen know this committee has for some time had a keen interest in this matter. I am sure the chairman has indicated this. I do not think the committee members have anywhere near an adequate grasp of the totality of this problem, what you are doing and what others are doing. I know that is true in my case and I suspect it is true for most of the members.

But getting back to the question you just mentioned of updating the population base, this is a fundamental option for all sorts of activities. The data base is presumably contained in the Census Bureau's file and should be updated with the latest current data. There should be a historical comparability base also and it should be available on a census tract basis, aggregated by all the jurisdictions. Along with population figures there should be other relevant figures.

Is it possible for FEMA to quickly access that data in the Census Bureau at the present time so relevant data from a remote area like the Mount Saint Helens area could be made immediately available to crisis managers in Washington in the event of a disaster there?

General LEWIS. I am not aware as to whether we have a computer terminal to access their data base. The responsibility for that information lies with the Census Bureau, and it would be our responsibility to get it quickly. We might physically have to go to their data base to get it. We would be able to do that.

I would like to turn that question over to Mr. Girard.

Mr. GIRARD. Does this mean, General Lewis, you have just pinpointed responsibility?

It is an excellent question, yes, we do have capability to look at that information and use it at the time of a disaster. We learned, for example, however, at the time of Three Mile Island, that be-

cause of the state of the information we had to do a great deal of interpretation. The Dime file, which I am sure you are aware of, has some of the properties close to Three Mile Island located in the middle of Lake Erie, which would not have been too helpful. We have worked very closely with the people at the Census to try to make census data more readily usable.

Mr. BROWN. What reasons do the census people give you for instance, the Dime file?

Mr. GIRARD. Problems with the Dime file arose during the previous administration.

Mr. BROWN. It goes back further than that.

Mr. GIRARD. It does; the only information I got from our people, Census may have told our folks, but I did not hear this directly from Census, they just had such a massive job, they were unable to get to this level of validation in terms of carrying out their mission of conducting the census. As a result we have had to, internally, prepare some programs to attempt to validate Census information, which of course is costly and time-consuming but very important to us.

Mr. BROWN. I became aware of the Dime file and the efforts being made to develop that system as an important working tool after the 1970 census. It seems to me after 10 years and a reasonable amount of experience that system ought to be perfected. You could almost build an MX missile in that period of time, and this is nowhere near as complicated as that.

There must be some reason why you cannot go to the Dime file and get valid information.

Mr. GIRARD. We are looking into the matter. We have our own software that we are using to validate those statistics. I cannot provide you an answer as to what the Census Department has done in this matter, sir.

Mr. BROWN. I am trying to get at an underlying point that the national requirements for emergency needs may be a powerful tool in the national emergency management capability. I could make the same point, I probably will not because of the time, as to what you could do in upgrading local management capabilities.

For example, I am vaguely familiar with a system called Fire Scope in southern California for emergency management during major fire episodes. They have within the capability of that system the ability to inventory every piece of firefighting equipment in the Southwestern United States, including heavy equipment, air tankers, manpower, and to call them up instantaneously on a computer. I do not know if that works better than the Dime file or not, but ostensibly that is their capability; yet that deals only with one small area of emergency management in the event of fires. It does not cover earthquakes or volcanic eruptions or major riots, but the system is such that all of that could be made into one compatible system it seems to me. Emergency management factors might be the compelling reason to do that, and with a very little expenditure of money. Certainly that should appeal to this administration; furthermore with a concept of how this could improve the national capability, and operation in accordance with that concept, we could do a great deal to improve the capabilities of local government throughout the United States.

Am I making this speech for a reason—does it convey a message? Am I wrong completely, or what?

General LEWIS. No. As a matter of fact your message is received, willingly and gratefully received.

We are aware of Fire Scope. We have worked with some of the people who helped develop Fire Scope. It serves other functions besides having data available. It serves to coordinate the activities of all those who would respond to emergency; for example, fire and police departments—it is a good model. The Forestry System helped to develop it.

Mr. BROWN. That is right, and they had their money to continue with the program cut out this year.

General LEWIS. I was not aware of that.

Mr. BROWN. We keep hoping something will come.

General LEWIS. While FEMA has the overall responsibility, we will assure that each of the agencies understands his responsibility to maintain its data base to meet national emergency needs.

Mr. BROWN. You want the information in the Census Bureau, the Dime file. You are not always too sure how good it is and you may not always be able to access the data needed in a timely fashion. This matter of course is of great concern in the Congress, and we have a variety of legislation aimed at overcoming duplication, overlap, and so forth. Yet that system is years from reaching a standard of excellence which is reasonable as far as Government is concerned.

When you move out of Washington into State and local government, the situation is much worse, yet the data contained at State and local levels will be vital to emergency management in a national disaster. Am I correct?

General LEWIS. Yes, sir.

Mr. BROWN. It seems that one thing leads to another, here.

Let us, for just a moment, dwell on the communications aspect. We hear discomfoting rumors from time to time that our great communications system may not be perfect in the event of an emergency, that it is subject to serious technological disruption and may cause us some problems; even the classified system, as I understand it.

Now one of the things that has always intrigued me is that in disasters, one of the most commonly referred to and reliable communications services is some ham radio operator stuck out in the wilderness with his own outfit. In other words, a survivable autonomous unit of some sort seems to be the most effective answer to this communications problem in the event of disaster.

You have talked about what you are going to do in handling the television stations. That is beautiful for predisaster purposes. What happens if they are all wiped out? Have you an adequate plan for a replacement communication system, or am I asking for classified information?

General LEWIS. You are, sir.

Mr. GIRARD. We would like to brief you and others on the committee on that, sir.

Mr. BROWN. I think it would be appropriate for the chairman to ask for a briefing, because you cannot separate the aspects of this

problem. This committee runs up against that in civilian applications in a number of different areas.

But we have the capability of putting survivable communication links anywhere we want, satellite communication and so forth—am I correct?

Mr. GIRARD. With one exception, sir; we need a heck of a lot of money to do it.

Mr. BROWN. We are going to spend that money anyway. The projections are that in the next 10 years, 80 percent of this country will be connected with cable TV interconnected with satellites. That is going to take place whether you like it or not. The question is whether it can be coordinated in such a fashion as to contribute to this country in the event of a disaster. I hope the answer is yes.

General LEWIS. We do, too.

Mr. BROWN. Have you thought of any more good questions?

Mr. GORE. I have thought of some more questions. I do not know how good they are.

Thank you very much, Mr. Brown.

We have seen in the Congress the value of graphic display systems; the Congressional Research Service, along with the Congressional Clearinghouse on the future, had a workshop on computer graphics. Are you including that in your analysis of what can be done to access the data and present it in a usable form?

Mr. CAMPBELL. Yes, sir, we are. That is an integral part of the total information system that we are looking at, as that gets into the whole theme of Dr. Baker's point. You can take advantage of the high transmission capability in that area and use the terminal as a buffer to bring it down for the human, and using computer graphics capability gives you a greater level of interaction for the human to look and get an awful lot of information very quickly without bringing it down to the 40 bits per second.

Mr. GORE. What role, General Lewis, did FEMA play when the missile incident occurred in Arkansas some time back?

General LEWIS. I was not a member of FEMA at that time. I am not prepared to answer that question. All of us are new.

Mr. GORE. Will you provide that for the record?

[The information follows:]

Following is a summary of the role played by the Federal Emergency Management Agency in the Titan II missile site incident which occurred on September 19, 1980:

The agency was first notified of the accident at the Titan II Missile Site on the evening of September 18, 1980, when Arkansas State officials alerted the FEMA Region VI office in Dallas of the fuel leak. When the explosion occurred on Friday morning, September 19, both the FEMA Regional Office in Dallas and the FEMA Operations Center in Washington, D.C., were promptly notified. During the following hours, contacts were established with State and local officials and the Department of Defense to obtain specific information about the accident and the presence of any offsite consequences. Around noon on September 19, a FEMA staff member from the FEMA Regional Office was on the scene at the Arkansas emergency operating center in Conway. In addition, a FEMA staff member was on duty in the Air Force Operations Center in the Pentagon to serve as a liaison between FEMA and the Air Force. FEMA continued to monitor the situation throughout the day until there was assurance that no offsite consequences had occurred and that none were expected. Therefore, FEMA did not participate in the actual notification and evacuation during the missile incident.

In the event of such an accident with offsite consequences, FEMA is responsible for coordinating the overall Federal response and for serving as the focal point for any Federal liaison and coordination with State and local officials. Had there been

any significant offsite consequences during this incident, FEMA would have responded accordingly.

Mr. GORE. Your testimony indicated the importance of continuity in government and particularly the survival of the Office of the Presidency. Why is the Congress always left out of that?

General LEWIS. Sir, I would rather not answer.

Mr. GORE. I would rather you did. You did not complete your answer.

General LEWIS. I do have an answer; however, I am not able to give it here.

Mr. GORE. I will respect that, but that response implies that there is an answer.

General LEWIS. Yes, sir.

Mr. GORE. And if there is an answer, it seems to me, it would be known by Members of Congress, and it is not.

General LEWIS. Sir, I am not able to answer that question.

Mr. GORE. Well, maybe we can set up a briefing that you can attend, but my point is, if nobody in the Congress is aware of any such plan, then it cannot be a very effective plan.

General LEWIS. When we use the term "continuity of government," we mean all government. We did single out the Presidency, but we are talking about all branches of government, at all levels.

Mr. GORE. But you understand my point, if no Member of Congress is aware of any plan to include the Congress in that effort, then it cannot be very effective. Maybe it is just my own shortcoming in not learning about this plan, but it seems to me that Members of Congress should know about that. I have participated in briefings with FEMA in the past where this subject has been discussed by others, and I will look forward to talking with you about that in another forum. From your experience, could you comment on the feasibility of employing airborne, mobile ground, and fixed communications in a coordinated fashion?

General LEWIS. I would like to turn that over to our technology expert.

Mr. CAMPBELL. It is very feasible, sir. It is also, depending on the size and magnitude of a disaster, a common occurrence in the 30 to 50 declarations which occur under the Disaster Relief Act each year. They could range from just putting in a number of telephones in a disaster assistance center all the way to flying in satellite terminals where the need is great, such as the flooding down in Texas. There was a great deal of mobile radios in the Appalachian flooding deployed a number of years ago, to the tune of 300 to 400 radios. These were distributed over a three-State, two-region area when the flooding was that intense.

Each communication requirement is sized to the magnitude of the disaster. Under the provisions of that act, the FEMA organization now has the authority to call in any kind of communications capability that is necessary, ranging from the common carriers, all ranges of common carriers, to all the assets that exist in the Federal community.

Congressman Brown's point earlier about the fact that we have a large capability out there in the amateur radios, the existing national plan that was developed under FEMA direction by the National Communications System has a particular portion in there

which requires and directs how the participation of amateur radios in the region and general locality will be managed in the event of any kind of major disaster situation.

Mr. GORE. Has FEMA played any role in the formation of the new communications legislation underway in the Senate and soon to be underway in the House?

General LEWIS. FEMA provided its comments to this ongoing action.

Mr. GORE. Were they in parallel with the National Communications System comments?

General LEWIS. In part. We confined ourselves to the need for a system to support emergencies.

Mr. GORE. Do you have any suggestions concerning R. & D. initiatives which American industry might undertake in order to develop information technology suitable for dealing with emergencies?

General LEWIS. We are not prepared to give the specifics on that now, but certainly, we are going to involve industry.

I alluded to a program earlier on emergency operations centers. We have another program that last year was funded at a million-dollar level for work that could have been used for new systems. We had applicants come in with requests that totaled \$5 million. Some of these would have reached out into R. & D. to obtain new technology. We will be pursuing this area very actively.

Mr. GORE. Thank you very much for coming here today. I appreciate your testimony, the thought you have given to preparing it, and look forward to working with you.

The next witness will be Mr. Robert D. Vessey, director, disaster services, American Red Cross.

It is good to have you with us. Without objection your entire statement will be included in the record, and we would like to invite you to proceed with any or all of it as you wish.

STATEMENT OF ROBERT D. VESSEY, DIRECTOR, DISASTER SERVICES, AMERICAN RED CROSS, AND PRESIDENT, NATIONAL VOLUNTARY ORGANIZATIONS ACTIVE IN DISASTER

Mr. VESSEY. Mr. Chairman, it is a privilege to appear before your subcommittee today to share with you the experience of the American Red Cross Disaster Services in regard to the role of information technology in emergency management.

Last night when I was looking at the witness list with my 12-year-old son, he commented that I was the only one on the list without a title. I hope you will not find the testimony I have to submit superfluous to the committee. I do not want to end up like Adlai Stevenson did when a lady commented after a speech, "Mr. Stevenson, your speech was just superfluous."

He smiled and said, "Yes, I intend to have it published posthumously."

She smiled and said, "The sooner, the better."

In the interest of time I would like to highlight some aspects of our testimony.

You commented on the fact that the Red Cross is associated with national voluntary organizations active in disaster. I would be

remiss not to emphasize that in our country there are many voluntary organizations that have been active in the field of disaster relief and planning and mitigation for many years.

In light of General Lewis' comments I think it important to recognize, although our prepared testimony does not, that two of the newest members in NOVAD are the American Radio Relay League and React, which is a nationwide CB organization. These two have served with great distinction on many disasters.

One of the purposes in NOVAD is to get these organizations together with local, State, and Federal government and plan together how we can be more effective in time of disaster.

Those of us involved in disaster preparedness and response need a large variety of information on which to base our planning and our reaction. We need to know quickly who—how many people, and what—how many homes, businesses, et cetera—are at risk or threatened by a given catastrophe. Data about the extent of a disaster, the damage to public utilities and other lifelines, roads and transportation lines, the number of casualties, et cetera, are needed so that we can quickly estimate how many have been affected after a catastrophe of one kind or another has occurred and what human needs have been created by the disaster. We need to be able to have that information available in such form that it is quickly available to all of those with a need to know.

Certainly, the technology for the storage and transfer of such information exists in many forms, and our Nation's technological capacity of establishing and maintaining such systems improves with every passing month. The problem is with the information itself. We lack the data bases needed to take advantage of what technology has to offer.

To illustrate, the University of Massachusetts recently mounted an extensive National Science Foundation—funded study of the long-range socioeconomic impacts of disaster. The study was based on the changes in population and housing stock in selected census tracts impacted by floods, tornadoes, hurricanes, other storms and earthquakes over a 10-year period. To identify the disasters, the university researchers photocopied 16,000 pages of Red Cross files, obtained information from the Weather Service, the U.S. Geological Survey, the then Federal Disaster Assistance Administration, the U.S. Army Corps of Engineers, and newspaper files. In spite of the mass of information, the actual physical boundaries of the various affected areas could only rarely be identified because each agency used its own form of information recording. None of them corresponded with the others. None of them included the specific data as to streets and other identifiable areas involved. All the computers in the world could not have solved the problem. In fact, the Natural Hazards Research and Information Center at the University of Colorado has had a conference on this very problem, and urgently recommended that action be taken to develop the kind of data base that modern information technology could make usable to disaster relief and emergency management agencies.

I would like to skip ahead a little bit to say that earlier this month, at a conference in Knoxville, Tenn., where Federal, State, and local emergency planners, Red Cross representatives, engineers, and experts from the academic world met to discuss ways of

mitigating, planning for, and responding to earthquakes in the eastern part of the United States, one work group after another emphasized the need for a computerized data base to provide the information needed for legislative and organizational actions which must be taken during the next 5 or 10 years. This information system would encompass everything from the results of vulnerability studies which are being initiated on a pilot basis by FEMA and the U.S. Geological Survey to resources inventories. Presently, there is no truly comprehensive listing of available resources—be they cots and blankets, portable toilets, or heavy-duty construction equipment—in any of the national information systems. One does need to be established.

When the information is acquired, it needs to be processed into a system that is easily accessible to all agencies who need the data for their daily work and their long-range planning. This will require a considerable investment of funds, and it is our recommendation that the Federal Government provide as much funding as possible in the budgets of the various Federal agencies involved, so this system can be established, the data base formulated, and dissemination of the information provided for. FEMA could coordinate this effort.

One further illustration will provide the subcommittee with an example of information-sharing problems that now exist. Last June, there was extensive flooding in the area south of Chicago. In attempting to determine what families might still need Red Cross help before the cold winter weather sets in, we asked the Small Business Administration office in Chicago, Ill., for a list of families who had been denied SBA loans. There were two problems. One related to the Privacy Act, which could have been easily resolved because those families who had also applied to the Red Cross had already signed releases authorizing us to obtain information about them from the SBA. The other problem was that of a shortage of clerical help to go through the files of SBA and pick out the cases where the application for a disaster loan had been denied. If the application information had been routinely computerized, the information would have been quickly available once the Privacy Act considerations had been resolved.

What we are recommending, therefore, is that Federal disaster-related agencies be provided adequate funds for computerizing their disaster operations in the field. Once this is done, the field computers could then be linked to a centralized system within FEMA so that field data could be swiftly available for analysis and needed actions on a State, regional, or National level.

Computers are not the only kind of information technology that can be important in emergency management and disaster response.

Our testimony goes on to describe an experiment we had with Comsat in 1977. Originally we had had during that period an exercise in Texas where we had been experimenting with the satellite in a hurricane situation.

When the Johnstown flood occurred, we moved that equipment to Johnstown, and for a period of 48 hours it was the only reliable means of communication out of Johnstown.

When you realize that the satellites can transmit telephone messages, teleprinter hard copy, facsimiles of maps and charts, slow-

scan television pictures, X-ray plates, actual TV coverage, and a variety of other kinds of information, their utility as part of the emergency management information system is not only obvious, but in some instances critical. It is our belief, therefore, that some means must be found to either provide a satellite for disaster and emergency management use or that some mechanism be devised so that an adequate amount of satellite time is dedicated for emergency use at a cost that is not prohibitive for agencies like the Red Cross and local or State emergency agencies.

Mr. Chairman, these are just some of the linkages between information technology and emergency management that we in the Red Cross can see. At a time when budgets are being closely scrutinized and many programs are being reduced or eliminated, we realize that it is unlikely that there will be expensive, new appropriations for such technology insofar as emergency management agencies are concerned. However, we believe it is timely to look at what technology does exist, what kind of data exists or can and should be obtained, how they should be gathered and integrated into the technological systems. If nothing else, a concerted effort by FEMA to develop a uniform disaster data reporting system that could be used by all disaster and emergency-related agencies will undoubtedly lead to more cost-effective utilization of existing systems and provide guidelines for prudent decisions about what technology should be added in the future. Development and implementation of such a data collection and reporting system should not be expensive, yet the resultant benefit to emergency managers could be tremendous.

I appreciate the opportunity to share our views on this subject with you today and would be happy to answer any questions you may have at this time.

[The prepared statement of Robert D. Vessey follows:]

PREPARED STATEMENT OF ROBERT D. VESSEY

Mr. Chairman. It is a privilege to appear before your subcommittee today to share with you the experience of the American Red Cross Disaster Services in regard to the role of information technology in emergency management.

First, a brief word of background, so you will understand the interest of the American Red Cross in this subject. One hundred years ago this month, the Red Cross—founded in May of 1881—became involved in its first disaster relief operation, forest fires in the state of Michigan. Since that initial response, which was based on newspaper reports and other information obtained well after the fires had actually occurred and the extent of human need became apparent, the Red Cross has been deeply involved in disaster preparedness and relief. Our role was formally recognized by the Congress when it granted the Red Cross its original charter in 1900. The Red Cross role as the nation's primary voluntary disaster relief Agency with a mandate from the Congress to provide assistance to disaster victims and to help take all possible steps to mitigate the effects of disaster, has been repeatedly reaffirmed by the Congress, most recently in the Disaster Relief Act of 1974 (Public Law 93-288). We coordinate our operations closely with government at all levels and have working statements of understanding with the Federal Emergency Management Agency—a new statement is about to be signed—and a number of other federal agencies, the military and the United States Coast Guard.

Simply stated, the Red Cross program is one of planning for and providing emergency assistance to victims of disasters of all sizes. Such aid takes the form of mass care—feeding, shelters, supplemental medical care, provision of blood and blood products, handling of welfare inquiries from anxious relatives outside the disaster area. (Also, the Red Cross will assist families with their individualized needs of an urgent nature while government disaster programs are being mounted following a Presidential Declaration of a Major Disaster.) When government pro-

grams are not available, the Red Cross cross may provide additional recovery assistance such as repair or rebuilding of homes, replacement of essential furnishings not already provided on an emergency basis.

It should be added that other voluntary agencies are also active in the disaster field and that many of them coordinate their efforts with those of the Red Cross and the government. Twenty such agencies, including the Salvation Army, the Mennonite Disaster Services, the Seventh Day Adventists, Catholic Charities, the Lutherans, the Southern Baptists, the Church of the Brethren, the Methodists, the National Association for the Advancement of Colored People, and B'nai Brith, are active participants in the National Organization of Voluntary Organizations Active in Disaster Relief. At this time, I am the national chairperson of NVOAD. Those of us involved in disaster preparedness and response need a large variety of information on which to base our planning and our reactions. We need to know quickly who—how many people—and what—how many homes, businesses, etc.—are at risk or threatened by a given catastrophe. Data about the extent of a disaster, the damage to public utilities and other life lines, roads and transportation lines, the number of casualties, etc., are needed so that we can quickly estimate how many have been affected after a catastrophe of one kind or another has occurred and what human needs have been created by the disaster. We need to be able to have that information available in such form that it is quickly available to all of those with a need to know.

Certainly, the technology for the storage and transfer of such information exists in many forms, and our nation's technological capacity of establishing and maintaining such systems improves with every passing month. The problem is with the information itself. We lack the data bases needed to take advantage of what technology has to offer.

To illustrate, the University of Massachusetts recently mounted an extensive National Science Foundation-funded study of the long range socio-economic impacts of disaster. The study was based on the changes in population and housing stock in selected census tracts impacted by floods, tornadoes, hurricanes, other storms and earthquakes over a 10 year period. To identify the disasters, the University researchers photocopied 16,000 pages of Red Cross files, obtained information from the Weather Service, the United States Geological Survey, the then Federal Disaster Assistance Administration, the U.S. Army Corps of Engineers and newspaper files. In spite of the mass of information, the actual physical boundaries of the various affected areas could only rarely be identified because each agency used its own form of information recording. None of them corresponded with the others. None of them included the specific data as to streets and other identifiable areas involved. All the computers in the world could not have solved the problem! In fact, the Natural Hazards Research and Information Center at the University of Colorado has had a conference on this very problem, and urgently recommended that action be taken to develop the kind of data base that modern information technology could make useable to disaster relief and emergency management agencies.

Another illustration relates to flood forecasts. The National Weather Service provides extensive projections of current and predicted river heights, how much over flood stage those projections are, etc. What is not provided, however, is statements as to how those forecasts related to existing flood walls or levees, which may be many feet higher than the official floodstage, and when the floodwaters will begin to move into streets and homes. At one time, the Weather Service published river by river statements as to what had happened during past floods. These were a useful guide for preparedness and gauging the needed response when a flood occurred. However, the statements were time-consuming and laborious to compile and ultimately the practice was discontinued. If such information could be compiled from Flood Insurance Administration maps, disaster reports, and other sources, and fed into a computer, with the information updated periodically on the basis of actual floods and data about housing, highway and industrial development, the available printouts would contribute immeasurably to the effectiveness of planning and the cost-efficiency of response.

Earlier this month, at a conference in Knoxville, Tennessee, where Federal, state and local emergency planners, Red Cross representatives, engineers and experts from the academic world met to discuss ways of mitigating, planning for and responding to earthquakes in the eastern part of the United States, one work group after another emphasized the need for a computerized data base to provide the information needed for legislative and organizational actions which must be taken during the next five or ten years. This information system would encompass everything from the results of vulnerability studies which are being initiated on a pilot basis by FEMA and the United States Geological Survey to resources inventories. Presently, there is no truly comprehensive listing of available resources—be they

cots and blankets, portable toilets or heavy duty construction equipment—in any of the national information systems. One does need to be established.

When the information is acquired, it needs to be processed into a system that is easily accessible to all agencies who need the data for their daily work and their long-range planning. This will require a considerable investment of funds, and it is our recommendation that the federal government provide as much funding as possible in the budgets of the various federal agencies involved, so this system can be established, the data base formulated, and dissemination of the information provided for. FEMA could coordinate this effort.

One further illustration will provide the subcommittee with an example of information sharing problems that now exist. Last June, there was extensive flooding in the area south of Chicago. In attempting to determine what families might still need Red Cross help before the cold winter weather sets in, we asked the Small Business Administration office in Chicago, IL, for a list of families who had been denied SBA loans. There were two problems. One, related to the Privacy Act, which could have been easily resolved because those families who had also applied to the Red Cross had already signed releases authorizing us to obtain information about them from the SBA. The other problem was that of a shortage of clerical help to go through the files of SBA and pick out the cases where the application for a disaster loan had been denied. If the application information had been routinely computerized, the information would have been quickly available once the Privacy Act considerations had been resolved.

What we are recommending, therefore, is that federal disaster related agencies be provided adequate funds for computerizing their disaster operations in the field. Once this is done, the field computers could then be linked to a centralized system within FEMA so that field data could be swiftly available for analysis and needed actions on a state, regional or national level.

Computers are not the only kind of information technology that can be important in emergency management and disaster response. Generally, computer systems rely on telephone lines, but telephone lines are not always available after a disaster. The lines are frequently destroyed, or the circuits so overwhelmed that in effect they become useless for extended periods of time.

The September/October, 1977 issue of *Pathways*, a magazine published by COMSAT, has an article that begins with the sentence, "Clara Barton would have been amazed". The article contrasted Miss Barton's rudimentary communications set up at the first Johnstown Flood in 1889 with the Red Cross use of an experimental COMSAT satellite system during the third major flood there in 1977. For several years, the Red Cross and COMSAT had been experimenting with a portable transmitter unit for emergency communications into and out of disaster areas. The third of a series of experimental tests was going on in Texas on July 23, when the flooding began in Johnstown. As the Texas test was being concluded on Saturday, July 23, the needs for the satellite transmitters in Johnstown were relayed to Red Cross and COMSAT. COMSAT quickly obtained permission from NASA and the Canadian government—co-owners of the satellite involved—for use of the satellite time for the real disaster. Saturday evening the transmitters were flown to Pittsburgh and on Sunday they were in place outside the Red Cross disaster headquarters in Johnstown. During the next 48 hours, until communications improved sufficiently in the Johnstown area, Red Cross used the COMSAT units to communicate outside of the disaster area and within disaster area itself where the system was tied into what amateur radio and telephone communications were available. When you realize that the satellite can transmit telephone messages, teleprinter hard copy, facsimiles of maps and charts, slow-scan television pictures, X-ray plates, actual TV coverage and a variety of other kinds of information, their utility as part of the emergency management information system is not only obvious, but in some instances critical. It is our belief, therefore, that some means must be found to either provide a satellite for disaster and emergency management use or that some mechanism be devised so that an adequate amount of satellite time is dedicated for emergency use at a cost that is not prohibitive for agencies like the Red Cross and local or state emergency service agencies.

Mr. Chairman, these are just some of the linkages between information technology and emergency management that we in the Red Cross can see. At a time when budgets are being closely scrutinized and many programs are being reduced or eliminated, we realize that it is unlikely that there will be expensive, new appropriations for such technology insofar as emergency management agencies are concerned. However, we believe it is timely to look at what technology does exist, what kind of data exists or can and should be obtained, how they should be gathered and integrated into the technological systems. If nothing else, a concerted effort by FEMA to develop a uniform disaster data reporting system that could be used by all

disaster and emergency-related agencies will undoubtedly lead to more cost-effective utilization of existing systems and provide guidelines for prudent decisions about what technology should be added in the future. Development and implementation of such a data collection and reporting system should not be expensive, yet the resultant benefit to emergency managers could be tremendous. I appreciate the opportunity to share our views on this subject with you today and would be happy to answer any questions you may have at this time.

Mr. GORE. In your opinion, is there a need to upgrade equipment centers?

Mr. VESSEY. I think they could be improved. There is a variance, I think, with the capacities of States' equipment, and particularly at the local government level.

Mr. GORE. Could you give some examples of where contingency communications systems have been effective during crises, and also some examples of where planned backup systems have not functioned satisfactorily?

Mr. VESSEY. To answer the latter part of the question, it is common in a large disaster for the normal kinds of communications to be affected and then even concern from outside the disaster area overloads the system and makes it impossible to function. For those of us in the Red Cross, we have utilized as the backup system the American Radio Relay League, the ham operators, very effectively.

We have for our own operational use, just for the local disaster area, a radio frequency reserved for the Red Cross which has been effective and reliable.

Mr. GORE. What sort of training aids, workshops, documents, et cetera, have proven most useful in preparing volunteer personnel for emergency roles?

Mr. VESSEY. We in the Red Cross take the position that the volunteer is an essential part of our organization, but we operate on the premise that the people we send out on a disaster have to know how to perform the functions we ask them to perform, so we make no distinction between volunteers and staff. But we give extensive training at various levels and we try to provide the opportunities for volunteers to proceed in a career ladder up that scheme as their skills and time make them available to us. In NOVAD, where we do joint planning with local organizations, we make use of voluntary organization, which is important.

Mr. GORE. You listened to the exchange I had with Dr. Baker at the beginning of the hearing. What is your reaction to that? Is that generally the direction we ought to be headed, or is that too far off in the distant future?

Mr. VESSEY. I see that as certainly being possible and achievable, but one of the concerns we have is that we see certain steps that can be taken—for instance, my reference to Federal agencies that are active in the field and FEMA giving leadership to having capability in the field to computerize some functions. That is a subsystem. The President does not have to know about it. But the American people would have a better service from their Government and it would be a more cost-effective way of serving without duplication if we could coordinate our efforts in the field more closely, using the available technology.

Mr. GORE. What subsystems would you single out for computerization on a routine basis? You referred specifically to the SBA

emergency loan file. I assume the Farmers Home Loan Administration loan file should also be computerized. What others?

Mr. VESSEY. In federally declared disaster the individual family grant program administered by the State is an important component because those have an important relationship, the SBA, the Farmers Loan Administration—I would hope a tie-in could be made with the Red Cross and its programs. I would hope a tie-in could be made also with the Flood Administration and flood insurance organizations. Some efforts have been made in that regard, but they need to be tied more closely together.

Mr. GORE. In your view, should FEMA take the lead in encouraging SBA, Farmers Home, the individual family grant people, the insurance companies, and the Red Cross, to move to computerized files?

Mr. VESSEY. Yes, I think FEMA has given leadership in the past and is trying to give that leadership now. Some of the difficulties that have arisen in trying to get such a system, part of it has to do with the commonality of reporting. Everybody has a different form, a different system, that makes putting that data together more difficult. It does not make it impossible. FEMA is now in the State and local programs undergoing an effort to do just that. It is sort of a combined application verification procedure which would not only share the information but reduce the paperwork burden of the individual disaster victim.

Mr. GORE. I suppose if that information were computerized and readily accessible in the aftermath of a disaster, many private voluntary organizations including churches and civic groups would be able to participate more effectively in providing help to those individuals and families that still needed it. As head of the National Voluntary Organizations Active in Disaster, do you agree with that?

Mr. VESSEY. Yes, I do. I think it would enable the volunteer sector to put their resources where the greatest needs were and not duplicate efforts of State and local governments or the Federal Government and make the best impact with the voluntary dollar or the voluntary contribution.

Mr. Chairman, I have one other point I wanted to make—

Mr. GORE. Before you go to that, let me just ask one more question in this area: How could the voluntary organizations coordinate among themselves a computerized data system that would be compatible, each with the others?

Mr. VESSEY. The need to do that in the voluntary sector may not be that great. The coordination of voluntary groups is important. As we develop, most voluntary organizations look to the Red Cross to give that leadership. We have in the Red Cross the capability of doing that and interfacing with the Government at all levels. That is how we would propose to do it, to take on the burden and share the information with the other groups.

Mr. GORE. Very good. What was the other point you wanted to make?

Mr. VESSEY. The only other point I wanted to make was that I was at a meeting of the National Emergency Management Association of which General Ott, who will appear here tomorrow, the president. There was a presentation by Hillary Whitaker of the

National Governors Association and she was pointing out again the need for commonality in reporting and urging States to adopt a common reporting form and reporting practices about disaster, because they do not now exist. I think this is another area of concern and another source of interest on the part of the States' concern to find a way to have a common data base so everyone can agree what the information is that is being entered.

Mr. GORE. We are going to move on in order to try to finish up on schedule. I want to thank you again for providing this absolutely critical perspective for the hearings that we are holding. Thank you very much for the time and effort you put into it.

Mr. Richard B. Foster is our next witness, senior director, Strategic Studies Center. We welcome you, and without objection we would like to have you go ahead with your presentation.

STATEMENT OF RICHARD B. FOSTER, DIRECTOR, STRATEGIC STUDIES CENTER, SRI INTERNATIONAL¹

Mr. FOSTER. Congressman Gore, members of the committee and distinguished guests, I would like today to complement the presentations given so far and those which will be given by discussing the higher levels of emergencies, those deriving primarily from our national security requirements and long-term competition with the Soviet Union and the instabilities arising in the outside world that affect the United States and their relation to national communications.

I would like to summarize some of the results of a recently declassified study of command control communications [C³] originally published in 1962. One of the lessons learned from it is that long-range strategic forecasts can be made with some degree of accuracy on such issues as the national security telecommunications system and future requirements to meet national defense needs. I have put into the record this formerly classified document, which was declassified after 17 years. SRI published the study in 1980 as a retrospective look at the problems of national command and control communications in 1962.

One given for such a study is that communications technology is perhaps the most dynamic and complex technology and communications systems the most important single national system affecting our security and the health and well-being of the Nation.

The first requirement for future defense communications needs is to preserve our unmatched, regulated national telecommunications system as a national asset. This system changes relatively slowly over time because of the overriding requirement for maintaining universal connectivity at all times. However, the problem of forecasting trends in telecommunications science and technology is frustrating. Technical changes come rapidly, but certain national policies and strategic factors change more slowly. As a system, the national communications system is so large and complex that it must change in an evolutionary way, even though we introduce new technologies, such as electronic switching, into the system

¹ The views herein reflect those of the author and not necessarily those of SRI International or any of its clients.

constantly to make it more efficient and useful to the users of the common carrier system.

In making the 1962 strategic forecast, we began with the fundamental geopolitical positions of the United States and Soviet Union. In 1839, Alexis de Tocqueville outlined the direction in which he thought the world would go and foresaw a long-term competition between Russia and America for the leadership of the world toward a universal order with remarkable prescience:

There are now two great nations in the world which, starting from different points, seem to be advancing toward the same goal; the Russians and the Anglo-Americans.

Both have grown in obscurity, and while the world's attention was occupied elsewhere, they have suddenly taken their place among the leading nations, making the world take note of their birth and of their greatness almost at the same instant.

All other peoples seem to have nearly reached their natural limits and to need nothing but to preserve them; but these two are growing. All the others have halted or advanced only through great exertions; they alone march easily and quickly forward along a path whose end no eye can yet see.

The American fights against natural obstacles; the Russian is at grips with men. The former combats the wilderness and barbarism; the latter, civilization with all its arms. America's conquests are made with the plowshare, Russia's with the sword.

To attain their aims, the former relies on personal interest and gives free scope to the unguided strength and common sense of individuals.

The latter in a sense concentrates the whole power of society in one man.

One has freedom as the principal means of action; the other has servitude.

Their point of departure and their paths diverse; nevertheless, each seems called by some secret design of Providence one day to hold in its hands the destinies of half the world.

Certainly this competition has occurred in much the way outlined by de Tocqueville. The nature of this long-term competition can be analyzed in terms of the full spectrum of conflict, from the lowest level of violence to the highest level of nuclear war. The control of escalation from crises to general nuclear war stresses the communications system in a unique way: Crisis control and crisis management must be centralized in the Office of the President no matter where he is or when the crisis occurs.

In the long term, the Soviets have proven to be far more predictable and their military systems more forecastable than those of the United States. For many years, the Soviet leadership and their military high command have been preparing a capability of fighting wars, ranging from ideological wars up to a general nuclear war that might be—from their point of view—forced on them as a result of competition with the capitalist world.

The Soviet concept of history is firmly grounded in Marxist-Leninist theory. From this theory and their view of external threats they have developed a political-military doctrine. This doctrine changes very slowly and is predictable in its application. The nature of the Soviet-planned economy also forces them to predict goals to be achieved by allocation of economic resources. The Soviets have also developed a general doctrine for the role of science and technology. They have emphasized the education and training of scientists and engineers, and an increasing share of their GNP is devoted to the science budget and to military R. & D.

This emphasis on R. & D. and concentration on military high technology has enabled them to change the military balance and catch up with the West. They are trying now to catch up in other

sectors, particularly in lagging productivity in capital and labor, for example in agriculture.

In a recent study we did for the National Science Foundation comparing United States and Soviet training and utilization of scientific and technical manpower we found that the Soviets had, in fact, increased their rate of growth in output of trained engineers and scientists at an annual rate of 8 percent or higher. Their increase in the military budget for research and development is at the rate of about 7½ to 8 percent a year, doubling every 10 years. By the year 2000, a third of their military budget may be in research and development. On the contrary, the U.S. R. & D. effort as a percent of GNP has declined by 25 percent, and the Soviet's has increased by about 1.8 percent in the last few years. The Soviets have also developed a broad allocation strategy based on a doctrine which they call the scientific and technological revolution. This doctrine was enunciated over 20 years ago, and was one of the easily forecastable efforts of the Soviet Union.

This high technology strategy for military forces has required a great deal of patience during the two decades it took for the Soviets to overcome the large U.S. lead in military technology in the 1959's and 1960's even at the expense of urgent technological needs in their civilian sector.

The Soviet broad strategy throughout this 20-year period was to maintain the strategic initiative but lower the risk of general war; they accepted mutual deterrence of nuclear war while they pursued initiatives elsewhere. Uprisings, popular wars, just wars of national liberation—these we have seen throughout the world, most recently in Latin America.

Some 20 years ago, the Soviets announced they would expand in vulnerable areas where there was a low risk of war because of a small U.S. presence. From Cuba as a proxy, it was possible to predict expansion into Central America and South America; support of Soviet proxies in Southeast Asia, in Africa and in the Middle and Near East were a part of that strategy.

The Soviet doctrine of nuclear war fighting on the other end of the spectrum also was outlined in the early 1960's and permitted a highly accurate forecast of changes in Soviet and United States deterrent policies. The policies gradually ranged from massive retaliation and mutual assured destruction to controlled war, with the possibility of a prolonged war in which only nuclear targets would be hit and cities would be spared to be used as hostages to prevent retaliation on one's own cities. This idea of multiple-option targeting—as you will see in Mr. Hoeber's testimony—was predicted in 1962; it evolved in 1980 as U.S. policy.

As this change in strategic doctrine for deterrence of nuclear war changed in theory and evolved in practice, the demands on telecommunications became much greater. The Soviets early realized the extreme importance of communications to serve the command structure for control of forces and nuclear weapons, and to manage a crisis. In 1961, Minister of Defense Malinovsky outlined the way future wars at a global nuclear level would be fought: he stated that communications junctions, everything which "feeds war," would be specific targets in future United States-Soviet wars. Since U.S. common carrier communications are fairly soft and are not

well defended, they can be attacked directly by nuclear weapons, or by electronic jamming, or perhaps a hand grenade might be thrown into a vulnerable overseas communications link. The U.S. national communications systems must be made less vulnerable to all forms of attack: We are not expending enough effort to do this.

When we looked at the problem of defending communications in 1962, there was considerable argument about what we were defending: Population—and we have a large population data base—industry—and we have a large industrial base—or some more abstract thing. We concluded that the primary thing to be protected and defended must be the basic political structure for continuity of government and continuity of the political processes under the Constitution that constitute this Nation. Any form of temporary national military command over the civil government was deemed to be totally unacceptable. Therefore, the continuity of the President as Commander in Chief and head of Government must be the first priority for our defense efforts and for secured Presidential communications. The question of Soviet targeting of the President and the national command structure became important.

In 1962, we found that the national command and its communications would be destroyed with less than 20 weapons. At the same time, it was determined it would take several thousand weapons to destroy future ICBM silos. This extreme vulnerability of the national command structure and its communications would not permit a nuclear doctrine which called for the holding of strategic reserves and for terminating a nuclear war short of total devastation. Therefore a better protected command structure and communication system was needed. It is still needed. In 1962 we also made a study of the vulnerability of the Presidential successors and of Congress on the opening day of Congress; a 10-megaton air burst would have at least a 50-percent chance of killing the entire Congress and all legal successors of the President.

It was obvious a new system had to be evolved to maintain continuity of Presidential leadership. We evolved the idea of dispersion of successors and the Presidential duty party. Each successor should have an assigned duty party.

As we go through the list, there are two Members of Congress in the succession list; to that extent, they must be protected as a part of continuity of Presidential command. In that sense the Congress must be included.

Mr. GORE. Only as certain of its Members may become a part of the executive branch.

Mr. FOSTER. Yes, the two under current law are the Speaker of the House and the President pro tem of the Senate as legal successors after the Vice President.

In 1932 we looked at the problem of getting supporting communications, and it was evident that the national security communications system would depend very largely on the national common carrier system, the one described by Dr. Baker. In 1962 we found no other solution. Today 85 to 90 percent of all Government communications depends on the national carrier system. As we look into the future, aside from an unlikely grant for a federally built system, this percentage will remain constant through the year 2000. We are therefore left with the need to build up the national

common carrier system to make it more reliable for national emergencies as well as for war. There is no hope of getting a federally built system to substitute for the existing system, which must be adapted for emergencies up to and including survivability for continuity of Government in time of war.

Today the problem is not technology in the national telecommunications system; rather, it is to update the Communications Act of 1934 and to help the executive branch to unite its own divided house on national telecommunications policy. The problem of maintaining our technical lead over the rest of the world and the Soviet Union—which is rapidly disappearing—is a separate problem. Increasingly, we suffer from foreign competition and a lack of good engineers and scientists to plan, build, and operate complex systems, and we are gradually falling behind. There is a growing asymmetry between the United States and the Soviet Union in the education of youth. The teaching of science and math needs critical attention, and it is a vital need to which your committee can make a notable contribution.

Thank you, sir.

[The prepared statement of Richard B. Foster follows:]

FORECASTABILITY OF NATIONAL SECURITY
TELECOMMUNICATIONS REQUIREMENTS

A Statement for the House Subcommittee on
Investigations and Oversight of the House
Committee on Science and Technology
29 September 1981

by

Richard B. Foster
Senior Director
Strategic Studies Center

I am delighted and privileged to have been invited by Congressman Gore to testify before this Subcommittee. The problems of science policy and the control over certain critical technologies (e.g. nuclear weapons) are too-seldom examined in a broad national strategic and policy framework, looking to the longer-range future. I hope we can assist your committee in this effort.

I will use my allotted time to examine some of the problems of strategic forecasting. I will use as an example a study performed in 1959-62¹ for the then Chief Signal Officer, represented by Harold Silverstein, who regrets that he cannot be here today serving on this panel; and undertaken as a joint project with Bell Telephone Laboratories, D. L. Miller, project leader, and SRI, where I was the overall project leader. We three have once again come together in the Strategic Studies Center of SRI, to work on the 1980's version of the same problem--and as you will see, it has not changed, too much in 20 years.

My Strategic Studies Center at SRI has developed methods of interdisciplinary research to address problems of national security policy and national strategies, including the political, economic, and military

¹ SRI International, "A Retrospective Look at Some of the Basic Issues Connected with National Command, Control, and Communications," based on a reprint of a declassified 1962 SRI/BTL study entitled "National Strategic Command-Control-Communications to 1975," and subtitled "C", final summary report, Vol. 1 prepared for the Chief Signal Officer, Department of Army, by R. B. Foster, D. L. Miller, et. al.

factors set in the changing environments of technology and international relations.

Communications technology is perhaps the most important key to the long-range survival of the country. Our national telephone system is the central nervous system of our nation. All nations have recognized the importance of their national telecommunications core network that enables all subscribers to talk to all other subscribers through universal connectivity and standards, and provides the basic means of national command and control communications (C³) for all national emergency, mobilization, and wartime situations. In extreme cases, the nation's survival could depend on a surviving, reliable, and enduring national telecommunications system.

One of the problems of forecasting trends in science and technology is that changes come so rapidly that a sense of frustration arises in attempting to make the forecasts necessary for any good policy or strategic planning. However, today I will illustrate that such forecasts can be made, that there are underlying strategic factors and trends in international relations against which the developments in science and technology can be measured and taken advantage of in a timely fashion. The underlying factor in international relations is, of course, the long-term competition and conflict between America on Russia, the free world and the socialist world. This competition will continue indefinitely.

In 1839, Alexis De Tocqueville foresaw this long-term competition between Russia and America for the leadership of a new world order with remarkable prescience:

There are now two great nations in the world which, starting from different points, seem to be advancing toward the same goal; the Russians and the Anglo-Americans.

Both have grown in obscurity, and while the world's attention was occupied elsewhere, they have suddenly taken their place among the leading nations, making the world take note of their birth and of their greatness almost at the same instant.

All other peoples seem to have nearly reached their natural limits and to need nothing but to preserve them; but these two are growing. All the others have halted or advanced only through great exertions; they alone march easily and quickly forward along a path whose end no eye can yet see.

The American fights against natural obstacles; the Russian is at grips with men. The former combats the wilderness and barbarism; the latter, civilization with all its arms. America's conquests are made with the plowshare, Russia's with the sword.

To attain their aims, the former relies on personal interest and gives free scope to the unguided strength and common sense of individuals.

The latter in a sense concentrates the whole power of society in one man.

One has freedom as the principal means of action; the other has servitude.

Their point of departure is different and their paths diverse; nevertheless, each seems called by some secret design of Providence one day to hold in its hands the destinies of half the world.

But before I summarize some of the more important factors of the previously referenced SRI/BTL 1962 C³ study let me quote from the preface of that study in order to give you the origin of the acronym "C³":

THE C³ PRINCIPLE

"Command-Control-Communications are an entity. Communications service Command in exercising Control over forces. The nature of Command and its objectives related to the forces it controls must be understood in order to derive requirements for military communications. This understanding must be carried throughout the entire process of planning, developing, implementing, organizing, and conducting operations. All persons engaged in this process - commanders, staffs, communicators - must share and act on the C³ principle. Only in this way can communications meet the needs of the commander of today and assure that adequate facilities will be provided for the commanders of tomorrow."

To say the least, this principle has not been followed in the past 20 years. We have invested heavily in weapons systems and military manpower, but far too little attention has been paid to providing survivable and

enduring C³ systems to support and control these weapons and forces.

First, a little background on the objective and scope quoted from the 1962 C³ study:

"The objective of the study was to provide guidance for the improvement of communications systems supporting the command control of national capabilities and resources ... and should cover the period, present through 1975."

"The study was conducted from a national perspective. In 1959 the Army was responsible for providing communications support either in whole or in part for 81 agencies. These agencies were included within the scope of this study. The constitutional responsibilities and functions of the President were taken into account which relate to continuity of government and to the command and control of globally deployed military forces through the military chain of command. Consideration was given to the ways in which the communications requirements, not only for national defense agencies but also for other government agencies such as the Department of State, should be fitted together to best serve world-wide national interests."

"The study analyzed the command-control-communications problem in relation to the entire range of the spectrum of conflict from crises in the cold war environment to general nuclear war. It considered United States national objectives and policy as compared to those of the Sino-Soviet bloc and a range of possible alternative United States policies and strategies for countering the Communist threat through 1975."

The point of departure for the study was a comparison of long-range U.S. and Soviet political and social systems, and the conflicting foreign and military policies. The U.S.S.R. was treated as an expansionist imperial power, the U.S. as a status quo defensive power. The international behavior of the USSR is more "predictable" than that of the Western democracies for several reasons. Among them are:

1. The Soviet leadership has developed a grand strategy, (not a "master plan") in which all elements of state power--economic, military, technological, ideological, political--are orchestrated to achieve long-range goals. The totalitarian Soviet system has as its objective the enhancement of the power of the state under the leadership and control of the CPSU; the Party

leadership in the Politburo must, by the very fact of their total control over all elements of state power, develop doctrines to carry out that grand strategy.

2. The Soviet leadership--the CPSU Central Committee, the apparatus of the State, and the military high command--apparently believe that a global (general) nuclear war can be fought and won for valid and achievable political goals. They have developed a set of requirements for the mission of victory in a global general war. These global strategic objectives are the same in peacetime as in war, in accord with Clausewitz' dictum that political aims of the state should be the same in peace and war.
3. Another thesis is that Soviet strategy and political-military doctrine are firmly grounded in their concept of history, using highly systematic methods with a foundation of dialectical logic common to all the theorists and practitioners. Political doctrine is centrally developed and monitored by the Central Committee of the CPSU. Domestic and foreign policies are blended in the Party's Central Committee apparatus and confirmed by the Politburo. External foreign threats from the "Capitalist West"--ideological ("counter revolutionary"), political, and military--are a necessary component of the Party's population control mechanisms. Doctrine changes slowly in such situations, and tends to persist over long periods of time.
4. Soviet economic behavior is inherently more predictable than that of Western democracies. The Soviet planned economy with command allocations to the military and science sectors lends a quantitative dimension to long-range strategic forecasts when the economic allocations are correlated with the official political and strategic doctrine. This presents a sharp contrast with the volatile Western democratic states whose domestic economic and foreign military policies tend to "zig-zag," to use a Soviet phrase, every time an election is held.
5. Finally, the most important Soviet national strategic effort has been in educating, and training scientists and engineers, and providing an increasing share of GNP to the science budget and military R&D.

Soviet statements and announced policies as well as trends in scientific and engineering training and employment and in R&D expenditures, suggest a strong drive to catch up with Western technology. This has been

a theme of Russian/Soviet policies since the 19th century, and in fact can be traced back to the reign of Peter the Great at the turn of the 18th century, but it appears to have escalated greatly in the past one to two decades. Observation of the Soviet military and civilian economies suggests that a disproportionate share of Soviet acquisitions of technology, both from external and internally generated sources, continues to be channeled to the military. Increasing U.S. recognition and concern about the Soviet military and economic growth and its implications for U.S.-Soviet competition/confrontation/conflict have had three principal foci:

1. Two decades of steady buildup of the Soviet strategic forces to what is believed by many to be superiority over the United States in the early 1980s, accompanied by continuing modernization and strengthening of the conventional (including chemical) forces, especially the Navy;
2. The problem of technology transfer, both licit and illicit, to the Soviet Union in apparent support of a determined program for qualitative catch-up with the United States;
3. Soviet economic problems including the lagging productivity, especially in agriculture of all major economic factors--capital, labor, and land.

A recent SRI/SSC study¹ concluded that the extent and pace of the Soviet efforts in both scientific education and in financing military and civilian R&D were much greater than corresponding U.S. efforts.

As early as 1969, the slowdown in the growth of labor supply and other economic inputs had persuaded the Soviet leadership of the necessity of turning to more "intensive" forms of economic development than had been the

¹ C. P. Ailes, F. W. Rushing (Summary Report), R. B. Foster, Francis P. Hoeber (Commentary), "Education and Employment of Scientists and Engineers in the U.S. and the U.S.S.R.: Summary Report and Commentary on Implications for U.S. National Security Policy," SSC-TN-ISR-15, SRI/Strategic Studies Center (May 1981).

case in the past. Brezhnev, at the December 1969 plenum of the Central Committee, stated that:

Henceforth we must rely above all on qualitative factors of economic growth, on the heightening of the effectiveness [and] intensiveness of the national economy ... This is becoming not only the main but also the only possible means of developing our economy and solving such fundamental socioeconomics tasks as the construction of the material, technical base of communism, the improvement of the welfare of the workers, and victory in the economic competition of the two world systems ... We have no other way. (Emphasis added.)

In formulating the Ninth Five-Year Plan (1971-75), Soviet leaders opted for a major program of importing advanced technology and equipment from the West as a source of gain in productivity and as a solution to the economic deficiencies and management problems evident from the past record. However, apart from placing increased emphasis on the acquisition of Western scientific and technological advances, Soviet doctrine and policy statements began to emphasize increased allocation to domestic research and development and raising the qualifications of the labor force. In short, if the state imports, technology, it must train people to absorb and exploit it.

In the development of the Tenth Five-Year Plan (1976-80), intensification of economic production was the dominant theme. The plan, which was referred to as the plan of "effectiveness and quality," was based primarily on "the acceleration of scientific-technical progress, the rise in labor productivity, and the improvement in the quality of work by all possible means in all sectors of the national economy." The emphasis on intensification of production is evident throughout the plan, especially in statements of objectives for the five-year period, including that of raising the qualifications and professional skills of workers. The theme of intensification of the economy remains prominent in the draft of the Eleventh Five-Year Plan (1981-85).

A few of the noteworthy comparisons from the referenced study are:

- o In 1950, the total number of natural scientists and engineers was about 20 percent greater in the United States than in the U.S.S.R.; by 1974 (the latest year of which data are available for the U.S.S.R.), however, the U.S.S.R. had over twice as many natural scientists and engineers as the United States. This change in the relative number of scientists and engineers in the United States and the Soviet Union was largely the result of the enormous increase in the number of engineers in the U.S.S.R. during this period. While in 1950, there were approximately the same number of engineers in the two countries, by 1974 the U.S.S.R. had over three times as many engineers as did the United States. In the natural sciences, while there were more than twice as many scientists in the United States as in the Soviet Union in 1950, by 1974 this discrepancy had become somewhat less pronounced so that there were only one-and-one-half times as many natural scientists in the United States as in the Soviet Union.
- o The average annual rate of growth of full-time-equivalent scientists and engineers engaged in R&D for the Soviet Union from 1961 to 1976 was about 8 percent, while for the United States it was only slightly over two percent. While estimates for 1960 indicate that the United States had more scientists and engineers engaged in R&D than did the Soviet Union, by 1976, depending on which estimate is used, the number of scientists and engineers engaged in R&D in the Soviet Union was from 1.3 to 2.3 times the number in the United States.
- o Since 1964, U.S. expenditures on R&D as a percent of GNP have declined from 2.97 percent to 2.25 percent in 1978, a percentage drop of about 24 percent. By contrast, the Soviet Union appears to have been increasing the emphasis on performance of R&D in the economy. From 1963 to 1977, the United States showed an average annual decline in expenditures on R&D as a percent of GNP of -1.2 percent, while the Soviet Union showed an average annual rate of growth of 1.8 percent.

The 1962 forecast of Soviet behavior began with a summary of objectives and strategy:

Communist Objectives and Strategy

"The major threat to the accomplishment of United States goals lies in the Communists' long-range objective of achieving dominance of the world. The Communists attack United States' and allied positions and interest across the entire spectrum of conflict; precise pressure points are calculated to exploit areas of greatest Western vulnerability. The revolutionary forces operating in the world today are creating what has been called a "systemic revolution." In addition to these "natural" revolutionary disturbances, the Communists have exhibited a talent for converting tensions, arising from any source, into conflicts promoting shifts in relative power positions. The Communist goals of world domination leads to a protracted struggle of ideological, political, and military systems. Lenin, Stalin, and Khrushchev all have recognized the long duration of the fight for power with the capitalist countries of the world. This indefinite duration of the struggle often goes unrecognized in the Free World. The Communist method requires patience. Mao Tse-Tung reduced the essence of this strategy of protracted conflict to 16 words: "Enemy advances, we retreat; enemy halts, we harass; enemy tires, we attack; enemy retreats, we pursue."

"At present, the Soviets no longer regard major war as an inevitable precondition to the triumph of Communism. For the time being, they are concentrating their effort on "wars of national liberation" and "popular" uprisings. They recognize and are acting on the need, however, to be prepared for war at any level of conflict. The Communists distinguish between world wars, limited or local wars, liberation wars, and popular uprisings. The classification of popular uprisings as war invites close attention. In past time, popular uprisings suffered from military and organizational handicaps. Future uprisings, if supported by the Communists, may be waged on a larger scale and may be run professionally within the framework of coordinated world strategy. Thus, the inclusion of popular uprisings under the category of war might be explained by a Kremlin decision to run such uprisings henceforth as major military undertakings and for this purpose to provide the necessary military, command, and logistical assistance to "revolutionary" organizations. Although preparing for a

¹ As in Cuba, for example.

wide variety of warfare, the Communists still appear to believe that there is a good chance of avoiding a general nuclear war and at the same time leaving their adversaries no other choice but appeasement or surrender. Soviet military doctrine thus comprises a mixture of the less violent forms of conflict with threats of general nuclear war. To carry out this strategy, the Soviet Union has sought to achieve a rounded military posture capable of sustained fighting over the entire range of armed conflict."

Figure 4 from the study illustrated directions of communist expansion, explained as follows:

Communists Expansion into Vulnerable Areas

"Guerrilla wars and counter-insurgency operations will increase the requirements placed on global communications. Illustrated on Figure 4 is the current and projected direction of Communist expansion into Southeast Asia, the Middle East, and the southern hemisphere, utilizing the techniques of "revolutionary" or sublimated wars. There are a number of important reasons for the Communists to concentrate their effort in these areas, as opposed to a direct thrust at Western Europe or the North American continent. Success of the Communist drive toward the objective of world domination requires a shift in the balance of power and world influence from the Free World to the Communists. Included in the Communist aims are (1) dominance in military capability, (2) control of the major portion of the world's land and population, and (3) acquisition of superior industrial capacity, superior technology (as in space), and superior economic and natural resources. Control of the major portion of the world's land area and population would provide major support to domination in military capability, (2) control of the major portion of the world's land and population, and (3) acquisition of superior industrial capacity, superior technology (as in space), and superior economic and natural resources. Control of the major portion of the world's land area and population would provide major support to domination in the other areas of interest. Expansionist pressures toward these vulnerable areas by the Communists involve a smaller risk of nuclear weapons employment by the

* The Soviets support non-Communist "wars of national liberation," as in Algeria, even though the Communists may not control the leadership of these revolutions. Their intention is to later gain control of the "liberated" nation.



Figure 4. Direction of Communist Expansion

Source: Reprint of 1962 SRI/BTL C³ study, p. 21.

Free World. The smaller risk arises from the lower value placed on these areas by the Western allies in relation to their own areas. With the attainment of significant nuclear capability by the U.S.S.R., it has been necessary for the Western allies to weigh the value of defending territories involved in Communist expansion before committing themselves to a defense by nuclear means."

"The areas indicated in Figure 4 contain the great bulk of the underdeveloped territories of the world, and the peoples of these areas appear to the Communist planners to be vulnerable to the promises of Communist doctrine. The Free

World's political influence in these areas is marginal, except in Latin America. Its military power, insofar as force deployment, command structure, and communications for all types of warfare are concerned, is relatively weak."

A forecast of the evolving U.S. deterrent policy was made, in large part based on the probable direction of Soviet nuclear war doctrine toward a war-fighting capability on a global scale. Although the date forecast for adoption of a controlled war doctrine -1970- was off by a decade, Mr. Hoerber's presentation on Pd-59 issued in 1980 closely parallels the definition of the 1962 study controlled war doctrine, as illustrated in Figure 3 from the study:

Evolving Deterrent Policy

"Since changes in United States deterrent policy have had, and will continue to have, a profound impact on requirements for the national command-control-communications system, a survey of our evolving strategic doctrine is in order."

"Brevity requires that the evolving deterrent policy be greatly over-simplified, and only those factors which affect communications requirements will be highlighted. Figure 3 illustrates the possible evolution of United States policy. In 1954, at the beginning of the massive retaliation policy, about 10 hours were required to alert and ready the force for the first pre-emptive strike. When the positive warning concept was adopted about 1960, the force had to react within a few minutes (6-15), before the United States

★

"Since this section was first written, Secretary McNamara made an explicit policy statement of the strategy of the controlled response in his June 16, 1962, speech at the University of Michigan, reported in the New York times of June 17, 1962."

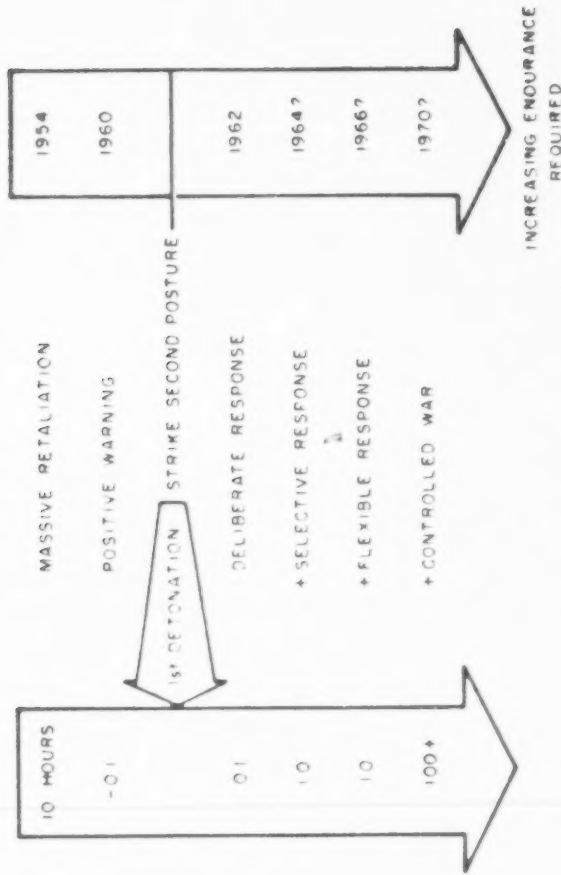


Figure 3. The Evolving Deterrent Policy

Source: Reprint of 1962 SRI/BTL C³ study, p. 19.

was hit. The survival of the force depended in large part on receiving positive warning of enemy attack via radar and making a Presidential decision (the "go order") before the national command structure could be destroyed and the force reduced by attacks on the bases."

"At present, a deliberate response doctrine (enunciated by the President and the Secretary of Defense) is being followed of not firing nonrecallable, survivable weapons, such as protected ICBMs and SLBMs, except in response to a direct attack. However, because of the present fragility of the national command-communications structure and a large part of the force, the decision to retaliate may have to be made in minutes (6-15) after the first detonation, if national command survives that long. By 1964 the United States may achieve the capability of a deliberate and selective response, making the retaliatory decision one hour after the first detonation of a nuclear weapon on United States territory. Selective response implies the ability to assess damage to the United States and NATO allies and to select the aggressor nations and types of retaliatory targets within those nations. Possibly by 1966 we can have a deliberate, selective, and flexible response; i.e., a response with the ability to retarget bombers and missiles held as a reserve force and otherwise increase the efficiency of our response either by delaying the retaliatory decision or by making a "re-strike" decision ten hours or more after an initial attack. Finally, by 1970 or so, the United States might have the capability of a controlled war - not only the ability to respond efficiently, but a capability to withhold reserves to deter further attacks or to carry out a series of exchanges over several days or months. At the same time, collateral damage to civilian populations in both friendly and enemy territory could be minimized."

"The more flexible our doctrine and the choices of action available to the President, the greater is the requirement for an increasing endurance as well as survivability of the command-control-communication structure related to the weapons."

"Inherent in the second-strike strategy and in the policy of deliberate, selective, flexible, and controlled responses is the desire to interject human deliberation and judgment into what otherwise might be an automatic operation (i.e., a preplanned "pushbutton" war). This would assure that the United States counteraction is in fact compatible with United States interest and objectives as they are viewed at that moment in history. Whether the United States response would be directed against a particular nation, against military forces, or against civil and industrial centers (or a combination of these) and what the level of response and the number of reserve weapons will be are aspects of the

national strategy. Decisions regarding these actions, though thoroughly studied in advance, must actually be determined during or after an attack on the United States."

"Post-attack civil actions are separate from but directly related to the military operations. These actions are essential to the preservation of the national political entity and the nation's ability to support potentially prolonged military operations. These actions require plans for continuity of government and communications facilities to implement them in parallel with the continuity of military command requirements. Thus it can be seen that the key to effective execution of the deliberate second-strike strategy is command and control, while communications are the nerve fibers which can make a strategy feasible."

The 1962 C³ study examined the Soviet threat to the U.S. national command system:

"Threat. An enemy may attack national command or its communications to prevent or delay or make ineffective the use of United States retaliatory forces. The requirement for survivability of command and command's communications stems from this enemy threat. In this study, the boundary condition of the worst case threat over the next 15 years was assumed to be Soviet ICBMs of increasing accuracy, warhead yield, and reliability. As to Soviet targeting philosophy, the validity of looking at communications as a target was reinforced by a statement on Soviet military doctrine made in October 1961, by Minister of Defense Malinovsky:

"War will both begin differently from before and will be waged in a different way. The use of atomic and thermonuclear weapons with unlimited possibilities of delivering them to any target in a matter of minutes by means of rockets makes it possible in the shortest period to achieve decisive military results at any range and over immense territory. The targets of crushing nuclear strikes, together with the groupings of enemy armed forces will be industrial and vital centers, communications junctions, everything which feeds war."

"Thus, in Soviet doctrine, communications are a specific target for general nuclear war. In Soviet military terminology, a command post is also a "communications junction."

Thus, for over 20 years, the Soviets planners have recognized the value of the U.S. national command structure and have made the national U.S. C³ system a part of their strategic targetting system. At the same time, they have constantly improved the protection provided then--the Soviet--leadership and the supportion of communications system. These facts were known in 1962, but we have been slow to improve our own C³ pasture so that we could fight and terminate a war, maintain a secure strategic reserve force, survive the nuclear attacks as a nation under the Constitution, and reconstitute our government and political and economic systems so that we might recover. All of these factors were included in the 1962 C³ study.

Figure 28 illustrates target options available to the attacker. Figure 29 illustrated the "attack prices" in terms of the number of nuclear warheads necessary to destroy the 1965 strategic structure, using weapons characteristics known in 1962. Note that there was a major imbalance in the attack price of weapons and the national C³ system. The most disturbing problem was the extreme vulnerability of the President, all of his successors, the Congress and the Supreme Court on Inauguration Day and on the opening day of Congress, illustrated on Figure 23. This problem can be solved, of course, by providing for assured survivability of legal President successors. The 1962 C³ study went on to say:

"Constitution. The need for survivability derives not only from purely military objectives but primarily from the higher level requirements imposed by the Constitution. These requirements are absolute in the sense that a compromise of any one of them involves serious and perhaps catastrophic changes in the basic national structure. One of the highest aims of our society is to insure that such changes be brought about only by statutory processes. the armed forces are constituted to protect the national political structure and the democratic processes that may be used to make changes within the framework of Constitutional authority. Logically, the use of these forces cannot be planned to contradict the authority in any way. Therefore, the Constitutional provision that the President is Commander in Chief was taken as a basic constraint of all solutions for achieving survivability of command."

"Strategic Doctrine. The evolving United States deterrent policy illustrated in the preceding chapters shows the

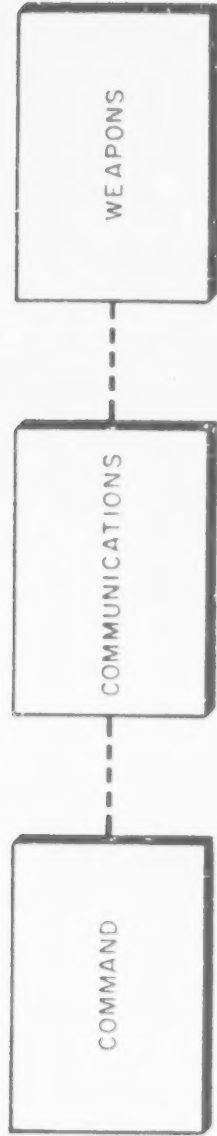


Figure 28. Target Options Available to an Attacker

Source: Reprint of 1962 SRI/BTL C³ study, p. 87.



Figure 29. Relative Attack Prices for the Strategic Structure - 1965

Source: Reprint of 1962 SRI/BTL C³ study, p. 88.

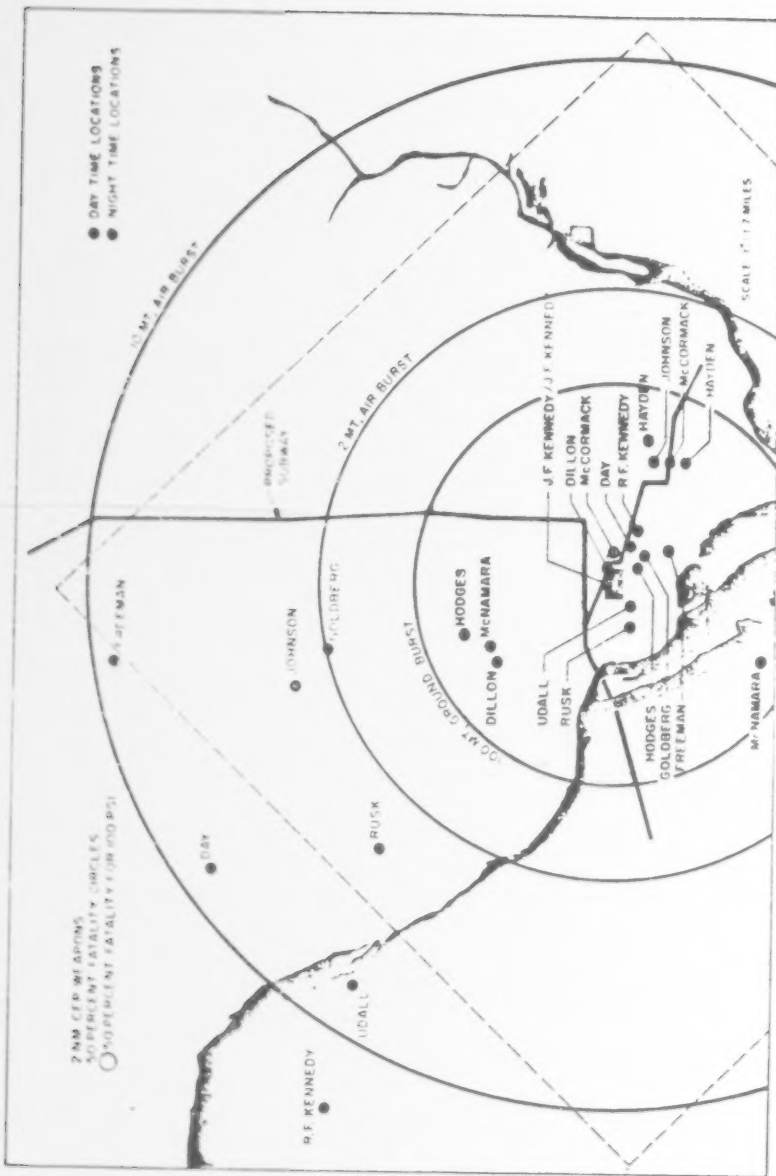


Figure 23. Vulnerability of Presidential Successors

Source: Reprint of 1962 SRI/BTL C³ study, p. 71.

sensitivity of command-communications requirements to changes in strategic doctrine. A reactive doctrine, based on a hair-trigger "safety catch" deterrent system, has few requirements for survivable communications need-lines and for endurance of presidential command. Current policy, requiring that the President be able to conduct military operations in general nuclear war beyond the first few minutes, radically increases the requirements for endurance of the presidential command function and the amount of information needed for deliberate decisions."

In order to meet these requirements for survivability of the Presidential function, a new concept was developed in the 1962 C³ study:

"A combination of deep underground shelters and active defenses would not necessarily give a high assurance of survival of the President or any of his successors within the present concept of relocation on warning and especially in the situation in which all thirteen presidential parties remain continually co-located and exposed on the surface. Neither will proliferation or presidential successors beyond the present twelve help much as long as everyone of them are in a concentrated area. Hence, prelocation is a requirement."

"Presidential Duty Party Concept. With the recognition of the present extreme vulnerability of the President and his successors, a concept of operations was devised that could increase the survivability of presidential command. The concept presents 13 presidential parties, one headed by the President and each of the other 12 by the legally designated presidential successors. Each successor would have a minimum staff to assist him in the assessment of the retaliation decision, in his actions as Commander of Chief over the surviving military forces; and in his civilian role as Chief Executive reconstituting the country for continuation of war, if need be. The size of these staffs was held to a minimum consistent with the deliberate decision policy, and the staff, or model presidential party, was divided into two groups as shown in Figure 24. The first echelon of the model presidential party involved in the military decision of retaliation would be required to be with their party leader immediately following the first nuclear detonations to aid him in making the retaliation decision. The second echelons, concerned with the

* With this concept of operations in a zero warning attack, active defense might have far greater value at the time of the attack than hardening, since it takes time to move people into a deep shelter.

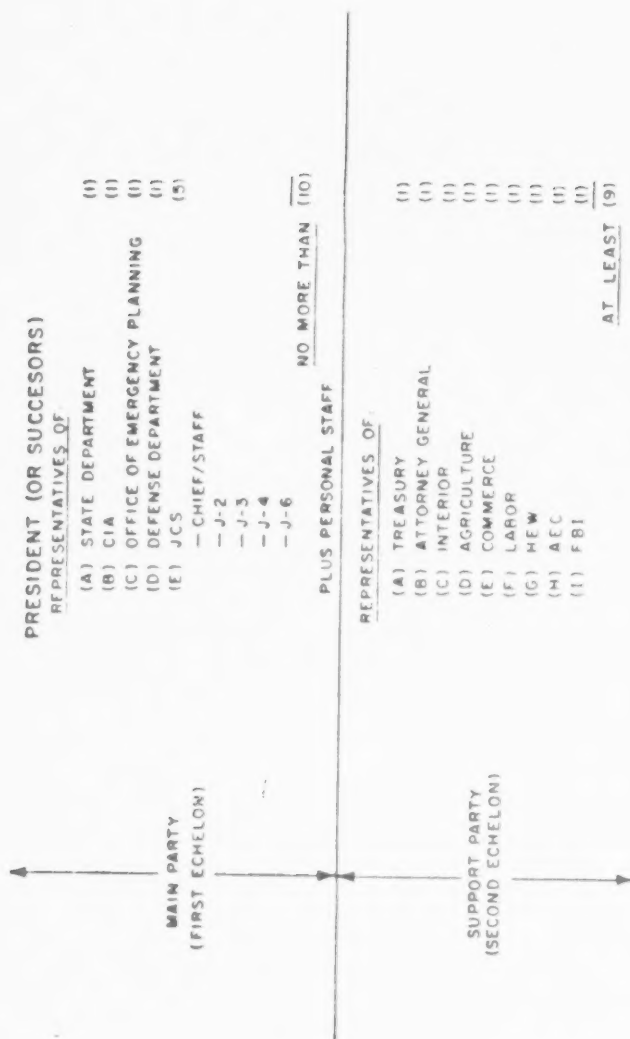


Figure 24. Model Presidential Party

Source: Reprint of 1962 SRI/BTL C³ study, p. 76.

reconstitution of the government, would not need to join their respective parties until after the initial military decisions had been reached and disseminated."

"It was concluded that one or more of the 12 presidential successors and the full first and second echelon staffs should constitute a "duty party" (or parties) at locations away from the Washington area at all times. This duty could be rotated through all of the 12 presidential parties so that each party need serve only about eight days each quarter. The locations should be chosen on a random basis and maximum security should be maintained. Such a duty party would serve three purposes.

- (1) Make the President an unattractive target to the enemy
- (2) Increase the probability of survival of Constitutional national command in a nuclear attack
- (3) Provide the opportunity to train the presidential successors and their staffs for both the military assessment and retaliation decision and the initial steps in reconstituting the government following an attack."

"The remaining presidential parties ("off-duty" parties) would, at the notice of actual or possible nuclear attack, proceed to predesignated locations as quickly as possible and prepare to act as the President and the national command until the senior surviving "President" was identified. Therefore, the first order of business after survival is to determine "who is President." This determination must be made at some specified time before the retaliation decision. For study purposes, 10 minutes before the H + 1 hour retaliatory decision was assumed."

The stress placed on the national telecommunications system by such a concept is self-evident. The surviving President may be anywhere in the continental U.S. and must have communications to perform all of his functions--first and foremost, as Commander-in-Chief to run the war, to conduct foreign policy, to direct the Government, and to lead the nation's

citizens. Three alternative concepts for a national security telecommunications systems were analyzed in Figure 35 from the 1962 study:

Concept Guidance

"The three broad alternate choices in approach for establishing a system concept are illustrated in Figure 35 and the consequences of each choice with respect to assuring the essential needs of command are briefly indicated."

"The last approach listed in the figure is the point of view that has developed since World War II with the advent of specialized weapons systems, new government agencies, and changes in the responsibilities of other agencies. In the absence of an over-all national command communications plan, there has been a tendency to build individual, single purpose communications systems for specific weapon systems and military and civilian missions. The result is a group of independent systems which have been neither planned in relation to each other nor, as a whole, designed to national command and control needs."

"The middle position in the figure describes the military systems that emerged from World War II. It also describes the nature of the commercial communications network from the viewpoint of military requirements. These systems met command's needs during World War II. Since then, with the many changes that have taken place in the military environment, special mission-oriented communications systems have emerged. Because these costly special purpose systems lack flexibility and have not proven adaptable to changes in weapon technology and strategic doctrine, attention has become directed toward pulling these and the common-user systems of each service together into one general common-user system. For economic reasons, this is a logical step, but in a general-purpose system which only incidentally serves command and control. A constant cycling has been created between the lower and middle alternatives, brought about by review after review of the situation, resulting in changes and revised objectives and return again to original ideas. This cycle continues because there are no established national command-control objectives and communications requirements toward which strategic communications planning should be directed."

"The first approach in the figure describes the way in which the essential command and control needs can be met; it is the recommended approach, substantiated by the research of this study. A system plan developed on the basis of this concept guidance would have the economic advantages of common-user utilization of facilities and can incorporate

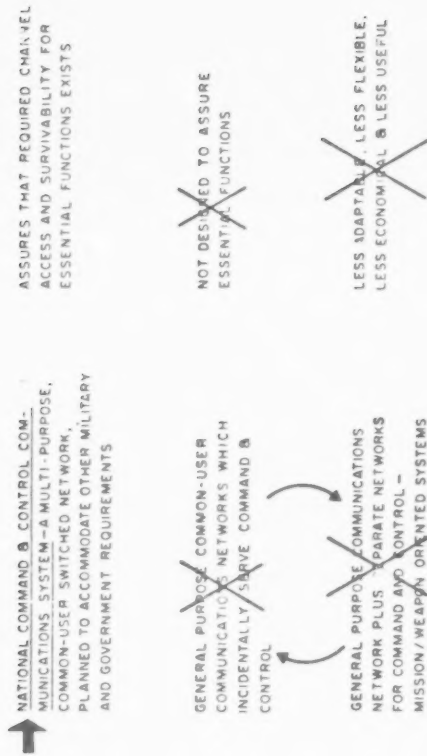


Figure 35. Alternatives for a Command-Control Communications Concept

existing plans into the system in the best arrangement for continuing use."

As you will note, this recommended concept is close to the current concept in PD-53 outlined by Mr. Hoerber. In other words, our national security telecommunications system depended then, depends today, and will depend in the future on the national commercial common carrier system adapted and strengthened to meet national security requirements. The common carrier industry, which includes AT&T with its long-lines departments, Bell Laboratories, Western Electric, and operating companies, along with about 1600 independent carriers comprise the national "core system" that is privately owned and government regulated--all other nations have publically-owned systems under the control of a government ministry or agency. The U.S. national security requirement has not been properly addressed in recent FCC regulations, court decisions, and certain government policies. There is a danger that our national "core network" that is the basis for any solution to the national security C³ problem today and in the future, will not be properly recognized in legislation. Cooperative joint planning by the Government (now represented at the national level by the National Communications System, or the "NCS") and the common carrier industry is a necessity if we are to preserve our regulated private enterprise arrangements which has provided what is accepted as the world's standard for technical excellence and service in a national telecommunications system.

The new communications technologies--such as protected satellites with mobile ground stations, advanced computer technology for switching circuits and terminals devices, and the new high-capacity terrestrial transmission systems, such as fiber-optics systems--will go a long way to help solve the major problems of survival of telecommunications in nuclear war. All of these developments have come out of the R&D laboratories of private industry, primarily the common carrier industry.

However, there has been a post-war tendency to let technology drive policy. The emphasis of new product-oriented policy has tended to destroy the integrity of the national system. But the national security needs in the broadest sense require a coherent national system.

The National Communications System (the NCS) backbone system (which is based on the private core system) requires NCS planning in cooperation with AT&T planners. The government depends on the common carrier (CC) facilities for most of its communications. These CC facilities must be altered to meet national security objectives in the backbone system. But while the relationship between government and AT&T may appear reasonable, questions are raised as to how the government planner for national security takes into account the other common carriers (OCCs), as well as government- and privately-owned facilities, in planning the backbone network. All the carrier- and government-owned facilities are useful in planning an NCS backbone system, but the "core system" has a unique quality because of its ubiquity and universal connectivity. NCS planners acting for the Government must develop relationships with the several public and private entities to create a backbone National Communications System. The Federal government derives 85% of its services from the public common carrier system.

Many of the services for the government are mission-related and should not be part of a larger system. Many are procured competitively from among the various common carriers and should probably continue to be on this basis if valid choices are available. In these circumstances, the NS/EP (national security and emergency planning) telecommunications system planner must deal with the departments and agencies to create a system concept that will include communications services that can be adequately provided by the common carriers and exclude those that have unique mission requirements.

I would only add two major recommendations:

1. The technology for solving many, if not all, of the national security telecommunications problems is at hand and in the laboratories. What is lacking is a clear set of national priorities, embodied in law and clear national telecommunications policies. The Congress has the main responsibility to update the Communications Act of 1934, to give specific guidance to its regulatory agency, the Federal Communications Commission, and to help the Executive Branch to heal its divided house on national telecommunications policy.
2. The technological lead we have enjoyed over the U.S.S.R. for almost 75 years is disappearing. The communications industry is the most highly technical of all our industries, and we have built and maintained the world's best telecommunications system. But this world leadership cannot be maintained without a much greater effort in the scientific and technical education and training of our young people.

The security of our nation requires that we address the growing asymmetry between the Soviets and the U.S. in the education of youth in science, engineering and mathematics. It is in this vital area that your Committee can make a notable contribution.

Mr. GORE. Thank you very much.

A lot of your presentation was on the strategic confrontation between the Soviet Union and the United States. I take it what you are saying there is that the course and direction of that conflict has made the emergency communications system in the military area very more important, very more critical; was that the thrust of your remarks there?

Mr. FOSTER. I had three points. The first and most important is that national command control communications, for the full spectrum of conflict, has been neglected for 20 years and it has received too little attention. It is just receiving attention today with the new National Communications System Agency and FEMA itself, as well as the Department of Defense.

The second point is that the national telecommunications system is a privately owned, Government-regulated common carrier system. This system is itself a slowly evolving system; it is the world's largest single system, and it is fairly predictable as to the directions it can take. It can be influenced by legislation, and should be. It is an area where legislation is badly needed, and the universal common carrier system should be protected as a national asset. It is not a product such as an automobile, it is a national service, and legislation is particularly needed here.

You mentioned S. 878 and others in which the Congress has a major role and on which I hope a series of hearings will be held on national security telecommunications needs.

My third point is that the technology we are depending on, including communications and technologies described by Dr. Baker, will run out of steam as we run into the barrier of fewer qualified scientists, engineers and technicians. We also appear to be getting fewer and fewer young people interested in science and technology. For example, in 1979, 97 percent of Soviet high school graduates had 1 year of calculus; in the United States, less than 5 percent has calculus. The Soviets place great emphasis on science education, and we have been deemphasizing it to the point where well-trained young people are disappearing.

Mr. GORE. I would note for the record that the chairman of our full committee, Don Fuqua, is holding hearings shortly on the manpower problems in the engineering field in the United States. This is critical, and I would agree with the comments you have just made.

Our Nation's first meaningful national commitment to improving the educational system in the country came, of course, in the direct aftermath of Sputnik, and the realization that this was a vital component of our national security effort. That coalition between right and left, liberal and conservative, which produced the first consensus and national agreement that we ought to move forward to improve our education system unfortunately appears to be dissipating very rapidly.

Mr. FOSTER. It has run out of steam.

Mr. GORE. And of course there is a lot of disagreement about the Department of Education and related issues, but there does seem to be an unfortunate lack of any sense of urgency about the ongoing decay of this national resource.

Mr. FOSTER. May I make this one comment on that, Mr. Gore?

Mr. GORE. Yes.

Mr. FOSTER. We are publishing a book based on studies for the National Science Foundation [NSF] called "The Science Race." We would like to make that book available in its present draft form to your committee. It has the greatest amount of unclassified material in this arena in the country. This resulted from 7 years of work, including discussions with Soviet scholars in the United States-Soviet binational arrangements monitored by the NSF.

There has been a kind of Sputnik shock which has happened slowly, without it being clear. We have come to the realization that the Soviets are sophisticated people in science and engineering. They have caught up with us in many of the areas in military technologies, and they are ahead of us in many scientific areas. The rest of the world is also catching up and pulling ahead. I mention Japan, certainly.

We have acted as though we can live off our scientific and technological capital forever. We have to replenish our human capital.

Mr. GORE. I might also note we have been busily educating scientists and engineers from other countries and we continue to freely export critical technology to other nations and to the Soviets as well.

Thank you very much for your excellent testimony here today. We certainly appreciate your perspective on this. It is of great help to us. Thank you.

Our next witness is Mr. Francis Hoeber, president of the Hoeber Corp. in Arlington, Va. If you will join us at the witness table. We appreciate your presence and without objection your entire text will be included in full at this point, and we invite you to proceed with your presentation.

STATEMENT OF FRANCIS P. HOEBER, PRESIDENT, HOEBER CORP.

Mr. HOEBER. Thank you, Mr. Gore.

I had some slides. I will refrain from keeping the committee in the dark and just proceed without them. They are in the handouts I submitted.

A picture may be worth 10,000 words, but I do not plan 10,000 words at this late hour.

Mr. GORE. You are welcome to show them if you want.

Mr. HOEBER. I want to use my allotted time for a brief review of what I perceive as significant changes in the national security environment that must be taken into account as we consider the problems of maximizing the usefulness of our exponentially growing communications, or information transfer, capabilities to support national security at all levels of emergencies. Mr. Foster—incidentally, a colleague of several decades in this work and a present client—has shown how many of these political and military developments were visible two decades ago. I want to pick up on where we stand today and what we need to do.

Let me start with a brief list of major Presidential directives governing the issues at hand. The list is certainly not exhaustive but will serve as a framemark for the discussion of the key points. You will note that the Presidential directives are presented in

reverse numerical and chronological order of issuance, but in what I think is a logical order of argument.

I am going to start with PD-59, which represents to me the culmination not only of the trends that Mr. Foster pointed out, but also of the long-predicted convergence of United States and Soviet strategic views. The only difference from the earlier expectations is that convergence has always been assumed to be their converging toward us, a very ethnocentric view. I think we have ended up much closer to them. Convergence is something like Irish neutrality. It depends on whom you are neutral again; this case depends on who converges toward whom.

But PD-59 was publicly briefed in August, a year ago, after some ambiguous leaks. Essentially, it set a new set of targeting priorities in nuclear war that emphasized first leadership; second, CounterForce—what I call CounterForce with initial capitals—against missiles, bombers, and C3I; and third, other military targets, or what I call counterforce, lower case, since I do not think we should distinguish the two in concept; and finally, war-supporting industries, which is very different from further development of the so-called economic targeting of a year or so earlier. This trend took longer than Dick Foster suggested earlier, but it started really on his schedule with the Nixon Foreign Policy Reports to the Congress, went on through Secretary Schlesinger and succeeding Secretaries in the evolution of flexible options, and includes one other element besides the targeting options I discussed, and that is a growing secure reserve force for the ultimate purpose of assured destruction for deterring the other side from attacking our cities or population.

In short, the new declaratory policy recognizes that nuclear war may, repeat, may not occur in spasm or big-bang fashion. I emphasize may, because I do not think anybody knows anything about nuclear war. We speculate about it. This is perhaps reflected in the positive tone in which many express opinions on it.

It appears increasingly possible, and therefore a contingency for which we must be prepared, that a nuclear war will be protracted, lasting perhaps months, conceivably many months, rather than the hours or days of earlier theories.

Equally important, it is quite possible and in my view probable that a war between the superpowers will come not out of the blue but out of a crisis conflict in which both sides have refused to concede perceive vital interests and are quite likely to be already engaged in conventional conflict in one or more theaters. We might therefore describe such a war as a prolonged war in which nuclear weapons are used.

I have used the word “declaratory policy” quite literally. The targeting categories named are not new but carry a new emphasis. Moreover, many changes just now beginning to take shape may be necessary before effective implementation is fully feasible. There will have to be new intelligence capabilities, new weapons characteristics, starting with survivability and endurance, and, of special meaning to today’s discussion, enduring command control communications and intelligence, or C3I, capabilities.

Prolonged war vastly increases the value of C3I, which brings us to PD-58, the continuity-of-Government directive, which stems logically from PD-59 and also from the changed strategic balance and

the nature of strategic weapons that brought about PD-59, I refer, of course, specifically to the shift from bombers to primarily ballistic missile threats.

It will be of little avail to have enduring weapon systems and even communications, which we do not yet have, if we do not have continuity of command to utilize these forces, including the capability to withhold them, as well as continuity to carry out other important functions of our national entity survival on a constitutional basis. That has been discussed and I will have more words on it.

PD-57 prescribes mobilization preparedness, as well as preparedness for war itself. Mobilization refers to preparation for all types of national emergencies but of course is viewed in particular in the context of mobilization for war.

PD-53 directed the National Communications System to support all the above functions, plus a number of others.

PD-41 made civil defense a national policy and is embodied legislatively in title V enacted in the fall of 1980 as an amendment to the Federal Civil Defense Act.

Now let me return for just a moment to the spectrum of emergencies which has been referred to throughout by FEMA and by Dick Foster, and let me shorten it to say that the responsibilities of FEMA start with natural disasters and manmade disasters, including terrorism. I would add the point that one great difference between these two categories is that natural disasters tend to occur statistically, from time to time—maybe occasionally two in a row, but they do not bunch.

Terrorism, which we have watched increasing over recent years, leads to the possibility that disasters might be widely coordinated, particularly if we ever get to the stage of nuclear terrorism. This makes a far more serious problem for FEMA—for the support of emergency or disaster mitigation and in maintaining necessary communications.

We go from there to international crisis and tension, and this is perhaps the central point, because such crises can lead to eventual war—conventional and tactical nuclear war—and I might include chemical and biological warfare—and finally the possibility of a prolonged general war in which strategic nuclear weapons are used.

Now, superimposed on this, and usually left out of the spectrum, is mobilization, which might start anywhere during the crisis period, and also which might not, since a President might decide for political reasons, both international and domestic not to mobilize.

Mobilization is often overlooked as an additional strain on communications. The increasing levels of conflict as we go from natural disasters to nuclear war are also accompanied by increasing stress on communications. Mobilization stresses communications in two ways. One, it is a version of what we see sometimes normally as simply a recovery or boom period in the economy, except that it comes very rapidly and tends to outrun the capability of the communicators, as well as many others, to expand facilities fast enough to keep up with it.

Second, and very specifically to the communications industry, there is superimposed the need for priorities, both for the Government and for industry, to meet the demands of the Government.

There is another set of dimensions in which the continuity of communications and information transfer is critical. That is in the functions of the Presidency that are the objective of the PD-58; I do not think we can elaborate in detail here, but the functions are quite clear. First and foremost, we must maintain the Presidency in order to maintain the Commander in Chief who can continue to prosecute a war. This means communications with the forces and also with the intelligence agencies. The President is, however, also head of state, and this means he must deal through the State Department with the enemy in the interest of controlling escalation, and seeking war termination; with allies, if we have any left, to keep them aboard and to coordinate military operations; and with other countries, which may cover a wide spectrum of problems.

The President is also the Chief Executive, and in wartime this really means his use of FEMA to run the priority parts of the Government. This may in war become ODR, the Office of Defense Resources.

He is finally, political leader, which means he must be able to communicate to the public. First, the President or the authenticated successor under the PD-58 procedures, must be able to go on the air one way or another and say, "I am here, I am legitimate; I am your leader; we are prosecuting the war, attempting to terminate it, to control it, or whatever the circumstances are; we will be paying attention to your needs, communicating such things as earlier mentioned, warning of fallout, and so on."

That is terribly important if you expect a country under nuclear attack to support continuation of the Government—continuation of the national entity, which is the ultimate objective.

Now, several things are omitted from this very brief sketch. One is that in each of these categories the Commander in Chief needs a whole structure of DOD and the intelligence community to look to its own endurance. The head of state needs the State Department and extensive, enduring, communications support. The Chief Executive, as already observed, needs FEMA/ODR to run those things which are essential and perhaps to forget about those things which are not essential until peace returns.

Also omitted, but not in my analysis, sir, are the Congress and the Supreme Court. I want one small Brownie point for that. It is not that we overlook the problem—and I empathize with Ben Lewis—it is simply that the Executive does not have jurisdiction over the Congress and the Supreme Court and therefore is limited in what he can do about arrangements for them, although there are cooperative arrangements which cannot be discussed here.

I would observe, as an aside, that there is one underlying point about the Congress, and that is that the President can call it into session, but he cannot send you home. You do that yourselves. If dispersal is an important aspect of protection of Members, that must be up to the Members and not the Chief Executive. But beyond that I do not want to go at this time.

There are also—if you think beyond protection to reconstitution—important differences among the three bodies: the Senate, the House, and the Supreme Court. The Senate, of course, can be reconstituted by appointments by the Governors; the House, by elections, special elections; the Supreme Court can be reconstituted by appointments, subject at some point to confirmation by the Senate.

This leaves finally the State and local governments, which are perhaps equally important. In fact, early on in a nuclear war they would be more important, because many things would have to start at the local level long before you could communicate or take time to communicate down the channels from the Federal Government.

The laws of succession in the States are very limited. In many of the thousands of local jurisdictions they are virtually undefined. Nevertheless, whoever survives in a nuclear situation is likely to take action, with or without full legal authority to do those things that cannot wait: to rescue, to remove debris, to put out fires, to give medical care, eventually to feed, and incidentally to provide water even before food. Those things would go on.

This highlights one of the great differences between the kinds of disasters that occupied much of this morning, local disasters, even where there may be a number of them in a terrorist situation. These tend to be islands of disaster, or islands of destruction in a sea of survival; in other words, within a country that can offer aid, that can offer resources, and that will have communications even if communications are locally disrupted.

At the other end of the spectrum, in a truly large-scale nuclear war, you may have islands of survival in what amounts to a sea of destruction, and the question of communicating among these islands will be serious. The original sense of the phrase, "lines of communication" was really "lines of transport"; getting not just messages but also aid to the islands of survival and the fringes of destruction will be equally difficult.

I might also mention that much reference was made this morning to satellites, and there is certainly no question of the communicating power of satellites; for example, in island hopping, they know no land barriers. But we must also take account of the fact that satellites are in the present state of the art highly vulnerable in a nuclear war. In fact, some plausible scenarios—all scenarios for nuclear war seem implausible to me—but some of the least implausible might start with attacks in space on satellites and possibly also attacks at sea, to change the balance of power, or the correlation of forces, for the simple reason that these attacks do not start collateral damage to the civilian people or economy and therefore may be nonescalatory at the outset.

Now, I have attempted a very rapid review to scope the breadth of problems with which national emergencies may confront the communications facilities and organizations of this country, and will also pose all sorts of other problems beyond the communications and transfer of information.

I will, therefore, use a little more detail on the provisions of PD-53, on communications, to recap and summarize these requirements.

The first requirement of PD-53 is connectivity with national command authority, to prosecute the war. In the view of SAC, this sometimes means "keep the President alive to give the 'go' code." If I had written the PD, I would have said to support the flexible execution of retaliatory strikes or to withhold them, which may be the most important thing to do at that stage.

The PD provides for retaining operational control of the rest of the Armed Forces, supporting military mobilization, supporting the vital functions of worldwide intelligence collection and diplomatic affairs, continuity of government during and after a nuclear war or natural disaster—of course, in the latter case, continuity of government is unlikely to be seriously in question—and supporting recovery of the Nation during and after a nuclear war or natural disaster.

Now the one other provision in the directive that is of interest to us here, and I think it was mentioned earlier, is that NCS is mandated to make maximum use of the common carriers as well as all available private and public communications systems such as those associated with railroads, pipelines, the FAA, and so on.

But this brings me back, finally, to Dick Foster's comments of the importance both qualitatively and quantitatively of the coordinating work of the principal, or dominant common carrier, A.T. & T. There are risks to the integrity of the core network and its availability for the building of a backbone network—a durable network responsible to national security needs—as a result of the tension between the national objectives of deregulation and competition for the general welfare of the economy on the one hand, and the necessity of providing adequately for emergencies, including war, on the other. Unfortunately, we have not fully evolved mechanisms for resolving these tensions and in my view for establishing when necessary the paramount of providing for the national common defense.

I cannot resist citing Adam Smith who, despite his belief in the overriding importance of the wealth of nations and in the superiority over State regulation of the hidden hand of a competitive system, did say that opulence must always give way to considerations of national defense.

I would like to close with one rather specific recommendation. What I have just said seconds Dick Foster's recommendation of attention to the revision of the Communications Act of 1934, which I am sure you all have already been deeply concerned about.

In the light of the breathtaking growth of technology in the communications field, including the inseparable information technology so eloquently described by Dr. Baker and with which you all are so deeply involved, one example comes to mind of a problem with which your subcommittee might be concerned and which may well require legislative action for solution. One of the latest revolutionary events in communications is the availability and imminent introduction on a large scale of fiber optics, or lightguide transmission technology—Dr. Baker referred to this as photonics—at least as revolutionary in its implications for both capacity and economy as the introduction of microwave transmission a generation ago.

The A.T. & T. recently applied for a construction permit for the first stage between New York and Washington of an Atlantic coast

trunk cable of optical fibers, presumably the start of an ultimately nationwide conversion from copper to glass, largely overlapping the period of putting all telephone lines underground.

In granting the construction permit, the FTC mandated open competition for both the supply of cable, repeaters, and related equipment, and the construction itself, with limited technical exceptions. It is not yet perfectly clear what this may mean if the orders must be given to an overseas low bidder.

In terms of the comparative advantage of economics, this may be in the national interest. On the other hand, if a major element of the communications system which we have been talking about is so essential in a wide range of emergencies and scenarios, one must raise the question of the reliability of foreign suppliers, a question raised between the two World Wars as to the availability of strategic materials, defined as those materials both essential and subject to sealane interdiction. Today, I would add political interdiction. There is in this case a potential transfer of capacity as well as of technology. I suggest that this is a problem for the attention of the subcommittee and for all those concerned with information technology in emergency management. I would also suggest that this is a case representative of a class of problems vital to the maintenance of mobilization preparedness and the mobilization base that may be solvable by legislative and/or regulatory policy without the direct expenditure of funds usually involved in adding elements of support of the mobilization base.

Thank you, sir.

[The statement of Francis P. Hoeber follows:]

THE CHANGING ENVIRONMENT FOR NATIONAL EMERGENCY PREPAREDNESS AND ITS COMMUNICATIONS SUPPORT

A Statement for the House Subcommittee on
Investigations and Oversight of the House
Committee on Science and Technology

29 September 1981

By:
Francis P. Hoeber
Senior Consultant
Strategic Studies Center

The views herein reflect those of the author and not
necessarily those of SRI International or any of its
clients.

Outline of testimony of Francis P. Hoerber before the House Subcommittee on Investigations and Oversight of the House Committee on Science and Technology, September 29, 1981

Introduction

It is an honor to have been invited by Congressman Gore to testify before this Subcommittee, and a privilege to appear before you all.

Start
I want to use my allotted time for a brief review of what I perceive as significant changes in the national security environment that must be taken into account as we consider the problems of maximizing the usefulness of our exponentially growing communications, or information transfer, capabilities to support national security at all levels of emergencies. Mr. Foster--incidentally, a colleague of several decades in this work and a present client--has shown ~~you~~ how many of these political and military developments were visible two decades ago. I want to pick up on where we stand today and what we need to do.

Let me start *with* (Chart I) with a list of major policy directives governing the issues at hand. The list is certainly not exhaustive but will serve as a framemark for the discussion of the key points. You will note that the Presidential Directives are presented in reverse numerical and chronological order of issuance but in what I think is a logical order of argument. *pos* (U) You will note also that they represent Directives issued during the last year of the last Administration. I believe they reflect the culmination of a decade of evolution in U.S. strategy, recognized in the last Presidential campaign and in the mandate given the new Administration. Whatever form new Directives may take, therefore, I think these provide a logical point of departure for our discussion of needs in this decade.

[PD-59, as you may all remember, was issued on 25 July 1980 and its general contents were briefed to reporters on 5 August. It deals with U.S. targeting policy, as developed in the 1978 DoD Nuclear Targeting Policy Study and reflecting the culmination of changes from the assured destruction-only concept of urban-industrial-targeting emphasis in

RELEVANT PRESIDENTIAL DIRECTIVES

- PD-59, WHICH IMPLIES THAT THE UNITED STATES MUST BE PREPARED FOR THE POSSIBILITY OF A PROLONGED WAR IN WHICH NUCLEAR WEAPONS ARE USED;
- PD-58, WHICH CALLS FOR PROJECTION AND ENDURING CAPABILITIES FOR PRESIDENTIAL SUCCESSORS;
- PD-57, WHICH MANDATES MOBILIZATION PREPAREDNESS;
- PD-53, WHICH DIRECTS NCS COORDINATION OF COMMUNICATIONS TO SUPPORT ALL OF THE ABOVE, AND MORE.

declaratory policy that had started with the early Nixon foreign policy statements to the Congress and the subsequent statements by Secretary Schlesinger and succeeding Defense Secretaries on the evolution of flexible options. The policy calls for increased emphasis on the targeting of enemy political leadership, nuclear forces, non-nuclear forces, and direct defense supporting industries. It also emphasized the importance of a growing secure reserve force (SRF), for the ultimate purpose of providing an enduring deterrent to enemy attack on U.S. cities and population. Thus, the new declaratory policy recognizes that nuclear war may, repeat may, not occur in a one-two or one-two-three spasm fashion, or what I call the "big bang." It is regarded as increasingly possible, and therefore a contingency for which we must be prepared, that a nuclear war will, on the contrary, be protracted, lasting perhaps months, conceivably many months, rather than the hours or days of earlier theories. Equally important, it is quite possible, and in my view probable, that a nuclear war involving the superpowers will come not out of the blue but out of a crisis conflict in which both sides have refused to concede perceived vital interests and are quite likely to be engaged in conventional conflict in one or more theaters. We might, therefore, describe such a war as a prolonged war in which nuclear weapons are used.

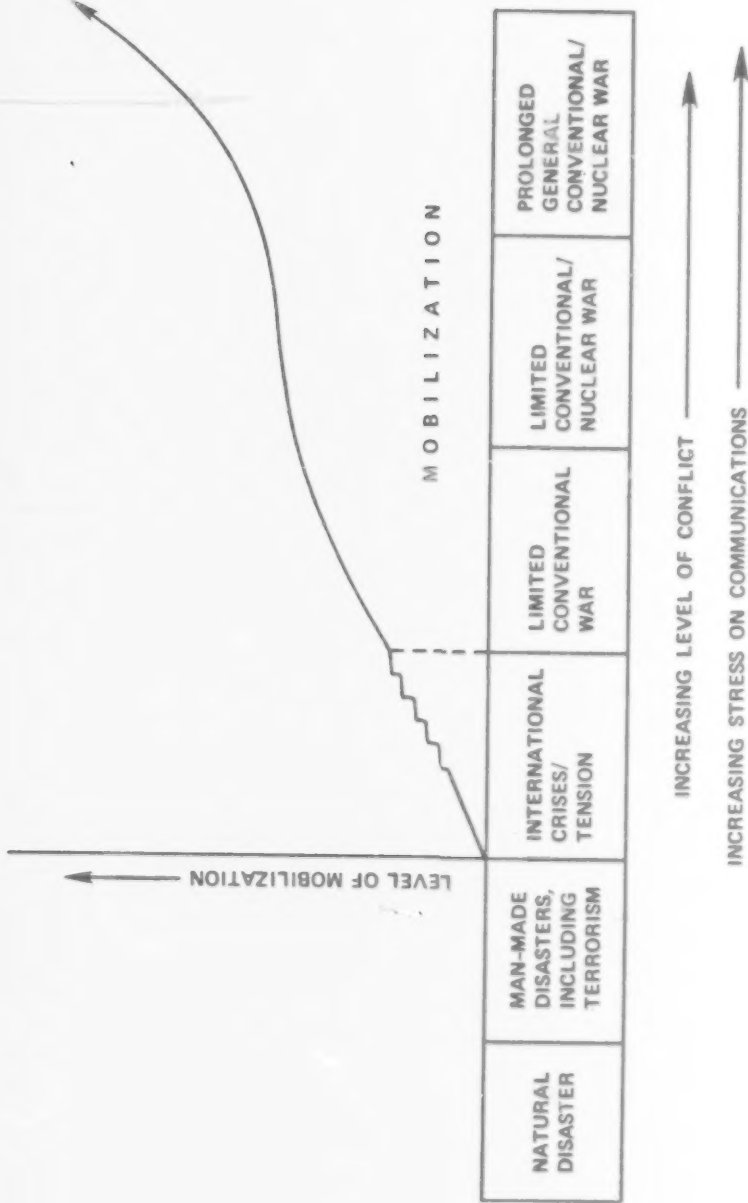
I have described this doctrine as "declaratory policy" quite deliberately. The targeting categories named are new only in their emphasis. Moreover, many changes, just now beginning to take shape, will be necessary before effective implementation is fully feasible. There will be new intelligence capabilities required, as well as new weapons characteristics, not the least of which is survivability and endurance, and--of special meaning for today's discussion--enduring command, control, communications and intelligence, or C³I, capabilities.

PD-58, the continuity of government (COG) Directive, stems logically from PD-59 and ⁰³⁵⁰ from the changed strategic balance and nature of strategic weapons that brought about PD-59. It will little avail us to have enduring weapons systems and communications if we do not have continuity of command to utilize these forces, including the capability to withhold them, as well as to carry out important other functions necessary for our national entity

survival on a constitutional basis, as will be discussed ~~on a subsequent chart~~. PD-57, and the Emergency Mobilization Preparedness Board being established by FEMA, emphasize the fact that we must not be concerned, as has so often been true in the past, with only worst case analyses of all-out nuclear war, but with preparedness for all types of national emergencies ~~(a point to which I shall return)~~. Finally, PD-53 directed the National Communications System to coordinate communications to ~~support all~~ ^{coord} of the above functions, plus a number of others. ^{Support all}

As I said, this list is far from complete, but it offers ^{a rich enough} menu for 20 minutes. It does not include, ~~for example~~, PD-41, ^{made} making civil defense a national policy and embodied legislatively in Title V enacted in the Fall of 1980 as an Amendment to the Federal Civil Defense Act.

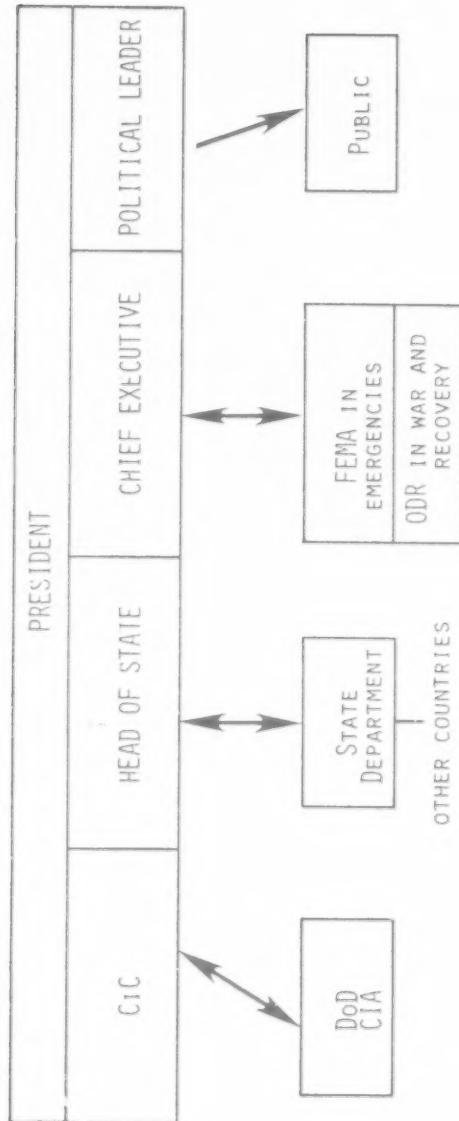
On Chart 2, I have attempted a simplified spectrum of national emergencies, starting with natural disasters, with which we of course have long experience, including knowledge of the fact that they always induce communications problems. Man-made disasters (used here in a limited sense, since after all war should be included as a man-made disaster) may increase in our complex industrial society and particularly as the possibilities of terrorism appear to grow, including the case in which terrorists might coordinate many simultaneous or near-simultaneous disasters (whereas natural disasters tend to be randomly distributed over time). From here we move to international crises and tension and the possibility that these may lead to limited conventional war, to limited conventional plus nuclear war (and I might have included chemical and biological in that box), to the ultimate worst case of a general conventional war in which nuclear weapons are exchanged between the superpowers. Superimposed on this diagram is the possibility of mobilization. The jagged start of the mobilization line is intended to indicate that mobilization may or may not precede the outbreak of war. This may be true for lack of warning time, or it may be because of a conscious Presidential decision involving considerations of escalation of tensions, domestic politics, etc. It is important to observe that not only the level of conflict increases as we move to the right but also the degree of stress on communications. It is often overlooked--though not in PD-53,



as we will see--that mobilization itself, even before or in the absence of war, stresses communications. It brings about the rapid escalation of demand that is also associated with an economic upswing, but at a much accelerated pace that may outrun the capabilities for facilities expansion. On top of the increase in aggregate demand for communications, however, is the necessity for greatly increased government and industrial priorities to assure access for messages of greater importance than those of a normal social intercourse, including non-essential commerce production.

There is another set of dimensions (Chart 3) for which information must be communicated with as much continuity as feasible in varying levels of emergency. As noted earlier, the continuity of the Presidency may be necessary in the first instance for the function of commander-in-chief, but the other functions are also of tremendous importance, since we need to provide in this country for far more than a military "man on horseback" in the even of an unwanted war. We must have a legitimate Constitutional President who can lead the effort to achieve survival of the national entity with its constitutional, political and social values preserved, not just the physical assets reconstructed. Of equal importance during a war will be the President as Head of State; in crisis and war communications with the enemy, allies and neutrals may be of paramount importance in escalation control, in seeking war termination, and in managing the crisis or war as well as possible pending such termination if deterrence does fail. The President is of course often referred to as the Chief Executive and the simple meaning of that is that he is also responsible for the running of the country; this may involve a smaller number of functions in a large emergency, but they will be vital ones. Finally, the President must be the political leader at all times. I have chosen to list this role separately here, but it is often called an additional function of the Chief Executive. At the right of our spectrum of conflict, nuclear war, it will be essential that the President or an authenticated successor be able to communicate to the public that "I am here, I am legitimate, you still have a government, we are endeavoring to both prosecute the war and seek war termination, you will be receiving information such as fallout warning as soon as possible, and soon ..."

KEY FUNCTIONS IN EMERGENCY AND WAR



The arrows on this chart indicate that communications problems start but certainly do not end with the Presidential level. DoD and the intelligence community, for example, must be able to inform the Commander-in-Chief of everything from the damage to the enemy to the state of his own union and forces; the Department of State must maintain communications with other countries, both for the use of the President and for a vastly greater array of communications about what is happening to our allies (if they still are) and third countries, which may of course choose to enter the war and which will wish to influence either to stay out or to support the United States. The communications requirements of FEMA and of ODR, when FEMA becomes ODR in war, are of course tremendously widespread and complex. In nuclear war they will vary as the conditions change from crisis to trans- and post-attack survival, reconstitution and eventual recovery. Not shown here, and probably beyond our available time are the many complexities involving both the Congress and the Courts as well as the connectors with regional, State and local levels of government. The latter are a subject in themselves, the scope of which may be indicated by a simple metaphor. In natural and limited man-made disasters, the disasters constitute islands of destruction or trouble in a sea of essential normality from which both communications and many forms of aid may be expected to succor the wounded and speed recovery. In contrast, in high-level nuclear war we may be faced with islands of survival in a sea of destruction, with difficulty for an undetermined period in even communicating among all of the islands. Clearly, in this extreme case, the functions of government and its aid in survival will start from the bottom up, with whatever people, organizations, and government authorities are surviving.

I have attempted in this brief review simply to scope the breadth of problems with which national emergencies may confront the communications facilities and organizations in this country. A little more detail on the provisions of PD-53 may serve to recap and summarize these requirements. That Directive (Chart 4) calls for the maintenance of connectivity between the National Command Authority and the strategic and other military forces for the execution of retaliatory strikes--and if I had written it I would have been very explicit that this includes the capability to withhold

NATIONAL SECURITY REQUIREMENTS FOR
THE NATION'S TELECOMMUNICATIONS FACILITIES
(AS OUTLINED IN PD/NSC-53)

- CONNECTIVITY BETWEEN THE NATIONAL COMMAND AUTHORITY AND STRATEGIC AND OTHER APPROPRIATE FORCES TO SUPPORT FLEXIBLE EXECUTION OF RETALIATORY STRIKES DURING AND AFTER AN ENEMY NUCLEAR ATTACK.
- RESPONSIVE SUPPORT FOR OPERATIONAL CONTROL OF THE ARMED FORCES, EVEN DURING A PROTRACTED NUCLEAR CONFLICT.
- SUPPORT OF MILITARY MOBILIZATION IN ALL CIRCUMSTANCES.
- SUPPORT FOR THE VITAL FUNCTIONS OF WORLDWIDE INTELLIGENCE COLLECTION AND DIPLOMATIC AFFAIRS.
- CONTINUITY OF GOVERNMENT DURING AND AFTER A NUCLEAR WAR OR NATURAL DISASTER.
- RECOVERY OF THE NATION DURING AND AFTER A NUCLEAR WAR OR NATURAL DISASTER.

execution, for whatever reasons and for whatever necessary period of time. Support is also necessary for the operational control of the rest of the armed forces. Support of military mobilization is mandated at all possible levels, as indicated in the earlier chart. Worldwide intelligence collection and diplomatic affairs, continuity of government in all circumstances, and support of the recovery of the nation from all emergencies are also mandated functions of the communications system. Finally, PD-53 mandates maximum use of the common carriers and of all available private communications systems, such as those connected with railroads and pipelines, and the public FAA system.

This brings us back to Mr. Foster's comments on the importance, both quantitatively and qualitatively, of the core network in which the AT&T is dominant. Mr. Foster touched on the risks to the integrity of that core network and its availability for the building of a backbone network, as a result of the tension between the national objectives of deregulation and competition for the general welfare of the economy on the one hand and the necessity of providing adequately for emergencies, including war, on the other. Unfortunately, we have not fully evolved mechanisms for resolving these tensions and, in my view, for establishing when necessary the paramountcy of providing for the common defense. For all his belief in the importance of the wealth of nations and the superiority over state regulation of the hidden hand in a competitive system, Adam Smith himself noted that opulence must give way to considerations of national defense.

In light of the breathtaking growth of technology in the communications field, including the inseparable information technology, with which your Subcommittee is so deeply involved, one example comes to mind of a problem with which your Subcommittee might be concerned and which may well require legislative action for solution. One of the latest revolutionary events in communications is the availability and imminent introduction on a large scale of fiber optics, or lightguide transmission technology, at least as revolutionary in its implications for both capacity and economy as the introduction of microwave transmission a generation earlier. The AT&T recently applied for a construction permit for the first stage, between New York and Washington, of an Atlantic Coast trunk cable of

optical fibers, presumably the start of an ultimately nationwide conversion from copper to glass fibers, largely overlapping the period of putting all telephone wires underground. In granting the construction permit, the FTC mandated open competition for both the supply of cable, repeaters, and related equipment and the construction itself, with limited technical exceptions. It is not yet perfectly clear, but this may well mean that the orders must be given to an overseas low bidder. In terms of the comparative advantage of Ricardian economics, this may be thought to be in the national interest. On the other hand, if a major element of the communications system we have been talking about as so essential in a wide range of emergencies and scenarios is to be available during these emergencies, one must raise the question of the reliability of foreign suppliers, a question raised between the two World Wars about the availability of strategic materials, defined as materials both essential and subject to sealine interdiction (and, today, to political interdiction). I suggest that this is a problem for the attention of the Subcommittee and all those concerned with information technology in emergency management. I would also suggest that this case is representative of a class of problems vital to the maintenance of mobilization preparedness that may be solvable by legislative and/or regulatory policy without the direct expenditure of funds for support of the mobilization base.

Thank you.

Mr. GORE. Thank you very much. We certainly enjoyed that. In the intelligence field, much is made of assembling what is referred to as "essential elements of information," readily accessed by analysts and other operational personnel. Do you find a parallel requirement in the civil sector handling of crises?

Mr. HOEBER. I certainly do. In any large-scale civil emergency, or in the civil portion of a war, we do not call it intelligence, but there are vast information requirements, which was the subject of much of the discussion with Ben Lewis, Bruce Campbell and company. If they need, for example, information on the distribution of population or the availability of other assets in and near Mount St. Helens, that is intelligence. That includes damage assessment, which is commonly an intelligence responsibility in the military field. In a nuclear war, the intelligence community and the military community will be preoccupied with both intelligence about what has happened to the Soviets, or any enemy, and what has happened to our own state of the Union and our assets. I think that is equally important on the civil side, and I would add that the data base problem may be no worse on the civil side but has been given less focused attention in the past and is less unified in terms of the capacity to communicate among the data bases.

Mr. GORE. As we focus on the role of information technology and emergency management, what would you recommend we include in a short list of the most salient issues needing attention, if you had to come up with a list of two, three, or four, or a handful. If I used the number three, what would you describe the most salient issues which we ought to address?

Mr. HOEBER. Three, as in triad?

Mr. GORE. Pardon me?

Mr. HOEBER. "Three, as in triad," what are the three most important—I do not know that I can narrow it to three. I would suggest that it seems to me, following my analogy that natural disasters and lesser manmade disasters occur in a sea of survival, that the things you really should focus on are those that are concerned with the more remote but vastly more significant contingency of nuclear war, the ultimate manmade disaster. And, of course, we are talking about the continental United States; nobody expects a war other than a nuclear war seriously to impinge on the homeland itself.

I think this is the area where you have to worry about the endurance and restorability of communications, and endurance includes the preservation of data bases and their availability as well as the ability to access them.

Now there is such a long list of specifics that it is very hard to say. One of the first problems of communications will be when power goes down and you have limited reserve auxiliary systems. In a nuclear war, the EMP effects are going to worry you.

As far as what you can do, it seems to me your legislation should maximize the opportunities for keeping intact the core network and the group that can organize and manage that, which is far beyond the capabilities of a tiny coordinating agency like the NCS.

Second, I think, in preserving that capability, you ought to consider in the legislation provisions that make it possible to pay for various kinds of protective hardening, against both blast and EMP, with emphasis on the EMP and the avoidance of "target areas."

Again, we talk as though we knew something about nuclear war. We do not know what target areas are, but we can say it is more likely that this building will be attacked than some other places, and it seems sensible to put cables, switches, and so on as far from target areas as you can afford to. Communications will be concentrated in cities for the same reasons that factories and even military facilities are concentrated in cities, namely that either you put them there because there is a city with an infrastructure, or a city grew up because you put some assets there. It is a chicken and egg question, but the correlation will always exist in an industrial society.

I do not know that that was "1, 2, 3," but those are areas of very major concern.

Mr. GORE. To what extent do you believe communications facilities would be targeted?

Mr. HOEBER. Per se, separately from collateral damage?

Mr. GORE. Yes.

Mr. HOEBER. Again, I do not know what the Soviets will target. We do have a great deal of information on what they discuss among themselves as useful to target, what fits their doctrine, and even what they do in exercises insofar as we adequately observe them. We do know that very high on their list is command control, which is most easily targeted and damaged by severing its communications. It does not do much good to have a commander with surviving capabilities, but not able to communicate with his troops.

So, I have to expect that at least major communications centers would be targeted.

Now there is also a long controversy in the open literature about whether the national command authorities would actually be targeted, and heads and seats of government. There is an argument, usually most loudly made, it seems to me, by those who think they know what nuclear war will be like, that, my God, you must keep the authorities alive so they can control the war and you can deal with someone for war termination.

I do not know whether or not that is true. As far as I am concerned, dealing with a decapitated, highly disaggregated Soviet Union, fighting off alligators on its periphery and even inside the country among nonsupportive republics, might be much easier than dealing with the current head of state in a war situation.

Therefore, I am not at all sure that the Soviets in this case may not well mirror image us and seek to decapitate the U.S. Government.

Mr. GORE. That is fascinating, and I certainly appreciate your presentation here today. Thank you very, very much.

Our final witness in this first day of our hearings is Dr. Stephen J. Lukasik, chief scientist with the Office of Science and Technology, Federal Communications Commission.

Doctor, welcome. Without objection, the entire text of your statement will be put in the record in full at this point, and we would love to hear from you.

Thank you for being here.

STATEMENT OF STEPHEN J. LUKASIK, CHIEF SCIENTIST,
OFFICE OF SCIENCE AND TECHNOLOGY, FEDERAL COMMUNICATIONS COMMISSION

Dr. LUKASIK. Thank you, Mr. Chairman.

I would like to make a few summary observations relating to my prepared statement.

Information is, of course, vital in any problem-solving situation. The problem-solving situation represented by an emergency implies three special characteristics of great importance to society requiring a rapid response and being a rapidly changing situation.

The information and the management authority needed to resolve crises are rarely collocated. Thus communication facilities are needed to link the human and information resources that must be brought together.

The communication problems and emergency management are of three types: Existing communication facilities may be degraded or destroyed; the crisis generates the need for more facilities than may have been present originally at the site of the emergency; and the crisis generates a great deal of secondary communications not directly related to the emergency management task, but instead following an attempt by people to secure information about the crisis so they can manage their own affairs.

Current and future technology, both at the hardware end and at the software end, can make significant contributions to deal with these problems.

My statement highlights a few of them, and earlier today Dr. Baker gave a wide-ranging survey of what the future holds for us. But as Dr. Baker pointed out, however vast the information available to a crisis manager and however rapidly one can access and transmit that information, one must still present the right 40 bits per second of information to the decisionmaker. This is both a technological problem, one involving the locating, analyzing, and formatting of the information for use, as well as the management problem: What to ask for and how to use the information to reach the necessary decisions.

These points are summarized on page 4 of my statement where I note that the technological revolution has been largely driven by commercial competitive marketplace forces. On the other hand, the evolutionary development in emergency management has been limited by funding and a priority status which may be perceived as overall inadequate and certainly highly variable from year to year.

Emergency management at all levels of government must exploit existing and rapidly developing communications capabilities. Certainly interest in having the most effective management capabilities is fostered by the kind of public attention that this subcommittee is giving to this important topic.

This attention should serve as a mandate to the private sector of corporations and individuals to join with government to seek out solutions.

Before discussing some of the technical problems and possible solutions, perhaps I should note the FCC role in the subject of this hearing. This is indicated on page 5 where it is pointed out that the Commission's role is not directed to emergency management but rather to the communications systems which support the manage-

ment function. We are regulators of the Nation's communications resources, we are not emergency planners or managers, although we would participate with several Federal and industrial organizations involved in emergency management.

There is, however, clear congressional guidance to the Commission that it should be mindful of emergency communication needs among other needs such as for the national defense when the Commission performs its regulatory role.

The Communications Act instructs us that our task is the regulating of interstate and foreign commerce and communication by wire and radio so as to make available so far as possible, to all the people of the United States, a rapid, efficient nationwide and worldwide wire and radio communication service with adequate facilities at reasonable charges.

As chief scientist of the Federal Communications Commission, I have responsibility for developing information on communications techniques and equipment on radio propagation and new uses for communications and for advising the Commission and its component offices on such matters.

My statement reviews some recent developments in the emergency communications system from a regulatory point of view.

In view of the lateness of the hour I will not go into these in detail but simply make reference, for example, to the illuminating experience of the Three Mile Island crisis which is discussed on pages 6 and 7.

Following Three Mile Island the Bell System, in connection with FEMA, the Department of Energy, the Department of Defense, the Nuclear Regulatory Commission, and the power industry, developed a prototype transportable communications system, a transportable satellite Earth terminal. But it is my understanding that funding for the procurement of this capability in adequate numbers is not currently assured.

In my statement on page 8 I discuss the FCC's recent actions in updating the restoration priority system regulations that are applicable to the Nation's common carriers. In addition, the Commission plays a role in spectrum management, including the licensing of land mobile radio systems for State and local government and private users. However, often the frequencies assigned for non-Federal Government use are not the same as those available to Federal agencies.

Two programs are mentioned in my statement to mitigate this problem of lack of connectivity between all levels of government. The FCC has also recently taken actions to assist State civil preparedness agencies in authorizing the use of high frequencies in civil disasters and emergencies. This is a region of the spectrum that has come into disuse for communications domestically. We have largely turned this region of the spectrum to other countries, developing countries particularly who find it useful, but we have made provision for the use of this part of the spectrum for domestic emergencies under controlled circumstances.

Another aspect is that the Commission is responsible for working with our AM, FM, and TV licensees to insure the viability of the emergency broadcasting system mentioned by General Lewis. This is reviewed on page 10 of my statement. Other subjects treated on

pages 11 through 15 include telex, load management, and traffic management in the public telephone system under emergency circumstances, the 911 service, both basic and enhanced, the information provided by the National Weather Service, the radio amateur civil emergency service that the gentleman from the Red Cross mentioned earlier this morning, and the activities that occur in the citizen's band radio service.

Finally, let me close with some remarks about the future, particularly with respect to networks of interconnected electronic computers. Such computer networks naturally give rise to the notion of information networks for two reasons: The computers in the network store large amounts of information, and the large number of users, each connected to their local computer facility are, by virtue of the interconnection of those computers, connected with each other.

A number of such computer networks exist, the first in the United States being the Defense Department's ARPANET, a network with which I have had some experience. Such networks have several characteristics that render them potentially useful for meeting emergency communications needs. These include the easy interconnection of different computers and different terminal devices, since one will never have standardization of this kind of equipment; the ability to reroute traffic around damaged switches; the ability to equalize traffic throughout the network for minimum delay in delivery of messages or data; and the ease with which different transmission channels, wire, line, radios, and satellite and the like can be interconnected.

You will be hearing from ARPA tomorrow, and so I will devote no further time to extolling the virtues of packet switch computer networks. The FCC has played a role in these developments by authorizing tariffs for such resale carriers in 1972 and by encouraging an active marketplace for the provision of customer-premises terminal equipment, for information services as a result of our computer query 2 decision, for the encouragement of competitive common carriers, and insuring their public connection to the information switch connection network.

There are, of course, two sides to everything. So on page 17 I note computer-based information networks are not by themselves the solution to emergency communications problems. I mention three: The need to interface often nontechnical decisionmakers to computer-based systems through such intermediaries as computer languages, programmers, analysts, and staff assistants. As a result the decisionmakers' needs may be redefined to fit the information system needs instead of the other way around. There is, in addition, the embarrassment-of-riches problem where the decisionmaker can be swamped by a massive data, raw, redundant, sometimes incorrect, often outdated. Again Dr. Baker's reference to the limited information absorption capacity of people is relevant. The last point that I make is the necessity of trading off wide-scale access to all data against the needs of personal privacy, confidentiality of information, and the protection of intelligence sources. To again quote from my statement on page 19, despite the manifest problems, the potential for information networks is difficult to overestimate. The flexibility that they apparently have to deal with

a variety of crisis situations is the reason that they can and will be very important to management and to national defense. Emergency communications must be less vulnerable to the disorganization wrought by crisis or disaster in order to be able to deal with these situations effectively. Information networks appear to have the potential to improve the situation not only in their increased survivability but also in their ability to provide capabilities when trying to ascertain facts in an emergency such as feedback, cueing sensors for additional, more detailed data, or permitting query-response-requery circles. The day may not be too far away when intelligent—that is computer-assisted—processed information via dynamic communications allow a remote and isolated decision-maker to bring order to a range of crises, domestic crises, statewide catastrophes, or nationwide emergencies. The technology is coming along rapidly. I am optimistic that emergency management can exploit these rapidly advancing communication technologies.

That I think completes the summary remarks that I would like to make, Mr. Gore.

[The prepared statement of Stephen J. Lukasik follows:]

STATEMENT OF

DR. STEPHEN J. LUKASIK

Mr. Chairman and Members of the Subcommittee:

I am very pleased to have this opportunity to take part in these hearings on the important subject of the role of new information handling technology in emergency management. Innovation in communications and information technology has been an important topic of personal interest to me, not only from my current perspective at the Federal Communications Commission, namely, a view of domestic communications, technology, and regulatory matters, but also from a perspective formed over the years within the national security community, where the management of crises and the technologies that support crisis management were, and still are, among the highest concerns.

INFORMATION NETWORKS FOR EMERGENCY MANAGEMENT--POTENTIAL AND PROBLEMS

I. PERSPECTIVE AND OVERVIEW

Information is essential in any crisis, ranging from small scale localized disasters, as many natural disasters such as floods are, to the most serious, large scale, wide-spread situation, affecting many people over extended geographical areas. Having the right information, in the right form, in the right place, at the right time is certainly the objective of emergency communications. Well, what's the problem? Where or what is the "devil" in all of this? What problem must emergency management personnel overcome in order to function and be effective? Well, frequently it appears that the crisis itself, which the emergency-management structure is attempting to control, at the same time is thwarting the emergency communications. It is simply a matter of restoring interrupted communications. It's also a matter of communicating when the conventional lines of communication are overloaded by the panicky public, seeking and sharing (mis)information and by the government, doing pretty much the same thing, but at the same time also attempting to improve the situation. Generally, the management structure, with its heavy dependence on emergency communications, has been just as vulnerable, if not more so, as the society or organization it seeks to manage under stress. The "devil" is the uncertainty, the disorganization, the chaos of the crisis itself. The emergency communications themselves are not immune to the crisis.

To illustrate the point, let me quote from a Washington Post editorial (December 15, 1978), titled "No to Civil Defense." I won't go into the main subject of the editorial, for it is obvious from the title, but I would like to quote a sentence in which the editors were suggesting that paper studies of

crises--in that case a nuclear war--do not even come close to what really would be the case in a severe catastrophe: "And the literature that holds otherwise, spinning out its clinical we-do-this-then-they-do-that scenarios is just that: literature--tidy imaginings of how the thing might go on paper, but surely not in bloody, rubble-strewn, irradiated, wires-down and switch-boards-out reality." (Emphasis added.) The communications outage has become a metaphor for the entire crisis itself.

There has been a revolution in communications (and in computing, but more on that later) since World-War II, when a bank of telephones or radios, linking on-scene observers to a "situation" board, maintained with a grease pencil, were the only tools available to a decisionmaker. The decisionmaker, usually isolated, remote from the crisis location, was frequently misinformed or received his information too late to act effectively.

Today the information revolution has made great changes possible. The revolution has provided us with developments, such as complex (possibly unmanned) sensors, wide-band data links, comprising thousands of equivalent voice-circuits, over disparate transmission media, from a variety of sources, along with advanced computational and display capabilities. The one element which has remained largely the same is the decisionmaker, usually isolated, still remote from the crisis location.

Let me advance the following hypothesis: the technological revolution, in particular in communications and in computers, has significantly outpaced the evolutionary growth in techniques for emergency management, in our appreciation of the problem within the Government and the population at large, and in material support of emergency management. In other words, if you will permit me an oversimplification, it just might be the problems are more people-driven, namely, what do we need to do? what do we need to find out? who is

in charge?, rather than technology-driven.

The technological revolution has been driven largely by commercial, competitive marketplace forces; on the other hand, the evolutionary development in emergency management, has been limited by funding and a priority status which may be perceived as overall inadequate and highly variable from year to year.

Emergency management in government must learn to exploit and work with existing and rapidly developing communications capabilities. Certainly, interest in having the most effective emergency management capabilities is fostered by the kind of public attention that this subcommittee is giving this important topic. This attention should serve as a mandate to the private sector--corporations and individuals--to join with Government to seek out solutions.]

As Chief Scientist of the Federal Communications Commission I have the responsibility for developing information on communications techniques and equipment, radio propagation, and new uses for communications and for advising the Commission and its component offices in such matters. In addition, I advise and represent the Commission on radio frequency allocation and spectrum usage matters. The FCC's charter in the area of emergency communications is explicitly stated in Section 1 of the Communications Act of 1934 (as amended in 1937) as a purpose for creating the FCC "...for the purpose of promoting safety of life and property through the use of wire and radio communication...." The same amendment added the following provision relating to the Commission in Section 4: "For the purpose of obtaining the maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the Commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and

coordination of these systems."

Thus, [the Commission's role is not directed to emergency management, but rather to the communications systems which support the management function. We are regulators of the Nation's communications resources; we are not emergency planners or managers, although we do participate with several Federal and industrial organizations which are interested in emergency management. There is clearly Congressional guidance to the Commission that it should be mindful of emergency communications needs, among other needs, such as for the national defense, when the Commission performs its regulatory role, namely, "...regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges...."]

In the following I will discuss two topical areas. First, I will review some recent developments in emergency communications systems--some large, some small--from a regulatory point of view. These will include such diverse topics as portable earth terminals for satellite communications for emergency use and the Emergency Broadcast System. After discussing these emergency communications developments as separate individual communications systems, I will address the second, broader topic, namely, information networks. The discussion will include potential benefits of information networks and also technical and operational lessons to be learned from information networks--composed of communications facilities (which are under the regulatory purview of the FCC) and computers (which are not).

II. EMERGENCY COMMUNICATIONS--REGULATORY DEVELOPMENTS

Emergency communications can be classified into three generic areas: communications among government entities, communications between the government and the public, and communications among members of the public. In each case, emergency communications needs are addressed by overlapping, yet in many ways distinct regulatory programs and technologies.

A. Government/Government

An orderly response to a local emergency demands that the involved federal, state, and local agencies coordinate actions with each other. This implies the need for reliable communications. Planning for emergency preparedness should, and does, include programs for facilitating communications. This means adopting programs that provide for communications paths between agencies before an emergency occurs and planning for methods of restoring damaged communications links during an emergency.

The need for prior planning is illustrated by the Three Mile Island nuclear power plant crisis that occurred in Harrisburg, Pennsylvania in March of 1979. Although the telephone service to the plant was provided solely by the Bell Telephone Company of Pennsylvania, the territory surrounding the plant was served by an additional three independent telephone companies. During the incident a high degree of cooperation existed among these companies. One can imagine, however, the difficulty in establishing additional telephone communications links if this had not been the case. In a five day period over 400 special services and facilities were installed at over 50 separate locations. These services were provided mainly for government agencies and the news media. Considering the magnitude of the problem, the telephone companies' response time was generally very good. Much time was consumed, however, by the ad hoc installation of cable. Indeed, in one instance it was necessary for Bell of Pennsylvania to run over 17,000 feet

of cable to provide an additional 100 voice channels. Although this was done as quickly as could be expected, in approximately 30 hours, a radio-based technology could have significantly improved this response time. Moreover, radio would have been immune to freak accidents such as one that occurred at Three Mile Island when, in a unrelated incident, a construction contractor severed a cable and interrupted communications to an observation post overlooking the nuclear plant.

After Three Mile Island, the Bell system, in cooperation with federal agencies such as the Federal Emergency Management Agency, Department of Energy, Department of Defense, and the Nuclear Regulatory Commission and representatives from the power industry, developed a communications system to satisfy requirements during local emergencies, the Transportable Emergency Communications System (TEX). This system would provide telephone stations at an emergency site and access the interstate network via satellite facilities. According to a Bell System report furnished to the Commission, TEX consists of a portable satellite earth station and telephone terminal equipment mounted on two truck trailers. Conceptually this equipment would be driven or flown to an emergency site where, within 12 hours, it would provide 192 voice grade channels and one television channel without the requirement of installing cable. Two scaled-down prototypes of this system were constructed, each providing 24 voice grade channels and one television channel. Although recent demonstrations of these prototypes to interested federal agencies and private companies have been very successful, funding for the program, approximately two million dollars, needed to proceed with the construction of the main system, is not assured.

Although a system such as TEX could provide a rapid solution to the loss of telephone communications during a local disaster, it would be a temporary solution. When a disaster such as an earthquake occurs, a large number of

landlines would be destroyed. It would be necessary to repair these circuits to restore normal communications. In conjunction with the National Communications System (NCS), the Commission has recently re-issued and updated regulations concerning the Restoration Priority System, which requires telephone companies to repair private leased lines according to the relative importance of the circuits to the national interest. Because the system addresses only private leased lines it affects mainly federal agencies. The system is administered by the Commission's Emergency Communications Division in conjunction with the NCS and to date 104 priorities have been granted by the FCC. This system should facilitate the orderly reconstruction of the federal telephone network after a local disaster strikes.

Land mobile radio systems play an important role during emergencies. They provide the main communications paths between control points, such as police, fire and civil defense headquarters and officials in the field. Moreover, federal agencies have their own radio systems to coordinate emergency operations. The FCC is responsible for licensing state and local government systems while the responsibility for coordinating the federal systems rests with the Interdepartment Radio Advisory Committee (IRAC). The IRAC is composed of representatives from many federal agencies, including the FCC as an observer, and is chaired by the National Telecommunications and Information Administration (NTIA). Generally, the frequencies available for state and local government use are not the same as those available for use by federal agencies. This can, and does, result in state and local agencies' inability to communicate with federal agencies in times of emergencies. There exist, however, two procedures to mitigate this problem. First, federal agencies can obtain a blanket authorization from IRAC to stockpile radios capable of operating on "federal frequencies" and to distribute them to involved state and local entities to be used in an emergency. This procedure

is frequently employed by the Coast Guard, when dealing with oil spills, and by the Forest Service, when fighting forest fires. Second, federal agencies can, after receiving permission from an FCC licensee such as a local police department, submit a request to the IRAC for authorization to communicate on "non-federal frequencies". The IRAC, with the concurrence of the Commission, would then authorize the operation. This procedure is used frequently by federal law enforcement agencies. As a final comment on government coordination, I note that only recently has FEMA joined the IRAC. This illustrates that alleviating federal, state, and local frequency coordination problems is still an area where work remains to be done, even though progress is being made.

The FCC recently took action to assist state civil preparedness agencies in coping with local emergencies. The Commission established a disaster radio response program in the Local Government Radio Service, titled "Operation SECURE", an acronym for State Emergency Capability Using Radio Effectively. Under this program, states, territories, and possessions may receive authorization to operate additional communications systems to provide an effective communications response capability in civil disasters and emergencies. Applicants would be required to submit detailed emergency communications plans to be approved by the Commission. A number of channels would be available for operation, all between 2 MHz and 10 MHz. State-wide communications would be possible because of the long range propagation characteristics of this part of the radio spectrum. The exact frequencies will soon be specified by the Commission via Public Notice. This should greatly improve the ability of state agencies to coordinate disaster relief efforts throughout the state from a single control point.

B. Government/Public

In addition to government-to-government communications, government agencies must be capable of communicating with the public especially immediately before and actually during emergencies. Examples are natural disasters, such as tornadoes or hurricanes, where there is generally some advance warning. The government should be able to warn the public of these impending disasters. In addition, public instructions should be disseminated during disaster relief operations. Let us not forget that not all communications are generated by the government; the public should be able to report emergencies, such as fires or explosions to the authorities so that they can effectively respond to them.

Probably the best known system for disseminating information in emergencies to the public is the Emergency Broadcast System (EBS). This system replaced an earlier warning system, CONELRAD, in 1964. EBS consists of a network of some 9000 voluntarily participating AM, FM, and TV broadcast stations, representing over 95 percent of all broadcast stations in the United States. Originally the system was designed to provide a direct communication link for the President to address the Nation in the event of a nuclear attack. In 1976, however, the system was modified to operate at three levels: nationally, statewide, and locally. Today the system can be, and has been, activated by governors, mayors, and state and local emergency management officials. Indeed, from the start of the program through September, 1979, EBS had been activated over 1100 times in state or local emergencies.

At the state or local level, EBS is activated by a telephone call placed by an authorized individual or agency to a predesignated FM or TV station. This broadcast station then transmits the activation message to other broadcast stations, which then retransmit it to even more stations, activating all stations in the affected state or local area. These stations receive the

activation message via radio and rebroadcast it to the general public in lieu of their regular programming.

The Commission has the responsibility for maintaining the rules and regulations for EBS, educating local broadcasters and officials in the use of EBS, and ensuring the integrity of EBS at the state and local level. Today, it appears that most of the country is covered by EBS and, judging by its use, it appears that the system has been effectively employed at the state and local level.

A relatively new concept in broadcast service may be used in the future for transmitting emergency messages to the public, called Teletext. Teletext is technology that superimposes textual and graphic information on a television signal in addition to regular programming. This additional information is transmitted in an "unused" portion of the broadcast signal and does not disturb the regular programming. With the proper decoder, television receivers may be used to view teletext signals. These signals can be used to caption regular programming, e.g., for the deaf; alternatively, the regular programming can be muted and the television receiver used as a textual display. In either case, the teletext signal could be used to send emergency information.

There are presently two technologies used for captioning: open and closed. Open captioning is used for transmitting text that can be received on any television receiver; no special decoding equipment is required. Emergency bulletins are presently broadcast over television using open captioning. Closed captioning, however, requires the use of special decoders to display the caption on the television screen. It is, in a sense, a very limited teletext system. (All of these systems have one advantage in their use for transmitting emergency messages--they can be viewed by the deaf.)

Teletext is only in the developmental stage, however and it could be some time before wide-spread implementation is achieved. In an item coming before the Commission, it will have to be decided whether to establish a standard for this innovative technology or to allow licensees the discretion to choose among several present systems themselves. In either case, the Commission could require that any system used have an override capability to transmit emergency messages.

The National Weather service transmits weather information on one of three channels which can be received at many locations throughout the country. These broadcasts include both routine weather information and warnings of adverse conditions. When weather conditions threaten in a particular area, the weather service transmits a special signal designed to trigger built-in alarms which have been incorporated in special receivers. This signal is followed by the broadcast of a bulletin, warning of dangerous weather conditions. The receivers, available for under \$100, provide a low-priced, earlywarning system for consumers.

Let us move away from the broadcast area and examine a common carrier system, which differs from the previously mentioned systems in that it allows the public to contact the government via telephone in case of emergency; this is the "911" system. The "911" system allows all emergency agencies in an area to be reached by dialing the single phone number "911". The service is offered by the Bell System at two levels: basic and enhanced. The primary difference between the two levels is that the basic service involves a single answering point. The "911" system appears to work reasonable well in large cities and small towns; but in suburban areas, where many municipalities are involved, implementation of the basic system has been slow. The chief problem has been reaching agreement on a common answering point among many different

local authorities. In spite of this problem, over 800 basic "911" systems have been installed. Presently this service is available to approximately 35 percent of the population.

In the enhanced "911" system, multiple answering points are used. Also, a number of additional features, such as automatic phone number and street address identification, are available with this more advanced system. However, only 9 enhanced systems are currently operating in the country, with an additional 30 systems being planned. The cost of the service, depending on options, varies from \$60 to \$100 per 1000 residences per month. The chief delay in the implementation of this service appears to be identifying sources of local funding.

C. Public/Public

The last portion in this discussion of emergency communications addresses communications among the public at large. Once the public is aware of an emergency, communication among themselves is a necessity and will continue throughout the state of emergency. Not only will people within the local area need to communicate, but also those not in the local area are likely to initiate long distance calls to the affected area. In some cases these communications are necessary and desirable, but they do increase the load on the common carrier communications systems, which already are be functioning at reduced capacity due to the emergency. Moreover, less important communications via the telephone system may block higher priority calls.

In an emergency the public telephone system may be un-usable in certain areas due either to physical damage to the facilities or to overloading the network with a large number of calls. Let us discuss each of these in turn.

The nation's long-haul network is composed of microwave and coaxial cable facilities, providing the long distance public telephone system, among

other services. In disasters such as floods or earthquakes, these facilities may be damaged, interrupting service. When this happens, telephone companies generally have two responses. First, the communications links between the switching centers may be rerouted electronically by using the spare capacity of the remaining facilities and by exploiting the diverse routing of the extensive facility network. The common carriers generally are able to restore affected routes within minutes for simple failures involving only a single route. Second, a crew might be dispatched to the site of the physically damaged facility. In some parts of the country, backup microwave towers may be employed in an emergency to replace damaged microwave towers. The common carriers can usually replace the damaged towers well within 24 hours. However, only a limited number of the backup microwave towers are available, whereas there are thousands of microwave towers in the long-haul network.

When a state of emergency is declared in a certain area and the telephone system is near capacity, the common carriers can exercise a number of controls for the public telephone system, in addition to the fixes to physical failure just mentioned. These controls allow the limiting of calls originating within the critical area. Moreover, long distance calls directed to the affected area can be blocked where they originate, preventing them from further loading the system.

If the telephone circuits in the affected area are still blocked in spite of controls, then key officials placing priority calls may do so by exercising voice precedence. This is accomplished by reaching an operator and verifying that the call is critical to the emergency. The operator can then secure a line and complete the call. These procedures are more fully described in Part 68 of the FCC's Rules and Regulations.

The Personal Radio Services may be able to supplement telephone

communications with radio communications. The Amateur Radio Service has historically been very active in assisting both the public and the government during local emergencies. Indeed, the value of the Amateur Service to the public, particularly with respect to providing emergency communications, is noted in the Commission's Rules and Regulations. Licensed radio amateurs may operate in the Radio Amateur Civil Emergency Service (RACES), if they are certified as registered in a civil defense organization. When telephone circuits are disabled or jammed, amateur radio operators may assist in providing either short or long range communications, including connecting calls into the telephone network by establishing a long distance contact with another amateur station outside of the affected area.

The Citizen Band Radio Service (CB) can also provide radio communications alternatives in times of emergency. Many CB groups have volunteer programs where they routinely monitor CB channel 9 to assist people with emergencies. Channel 9 may be used only for communications involving emergencies or traveler assistance, but emergency communications have priority at all times on all channels. Many police departments now install CB radios in their vehicles so Citizen Band licensees may be able to communicate directly with local authorities. In this manner they may be able to assist both the public and the authorities during a local emergency.

III. INFORMATION NETWORKS

Let us change gears now and address the broad topic of information networks and their potential impact.

A. Characterization

Broadly defined, an information network is a set of widely distributed nodes where data are generated or stored, where computer processing and

manipulation of the data, are performed, and where processed information is displayed for consumption. One (minimalist) point-of-view is that the network is merely a collection of nodes where information is either originated or received and where the communications links are only the necessary and invisible ties between these nodes. Interpreted more broadly, the information networks, including the people who interact with and through the network, are viewed as an entity--where communications are an integral part of how (and how well) the system functions. The communications links are "managed" or operated upon by the nodes just as the data are to the best advantage of the entire system (for example, choosing the fastest path or the least crowded or the least physically vulnerable route). It is in this flexibility that information networks can be seen as relevant and critical to emergency management. The development which has made information networks a reality is the rapid growth of high-speed and relatively low cost computers which can access large amounts of stored information.

An example of an information network is the Defense Department's ARPANET--where a user at a computer terminal in one part of the country has access to many internettted computers throughout the country and where the user's messages (i.e., data or programming instructions) to the computer are divided into smaller "packets" of information, transmitted via diverse common-carrier paths, and re-assembled at the destination by the computers of the network in order to achieve features such as efficiency (e.g., minimal delay en route) or reliability (e.g., high probability of receipt).

Other less dynamic examples of information networks include intelligence or military command centers, internettted with communications including different kinds of voice circuits, (i.e., encrypted and non encrypted), data communications, teletype, facsimile, and the like. In such information

networks computers can access information, such as weather data or the location of ships, maintained in a computer-compatible data base and display the information, suitably processed, to a decisionmaker at another location. The communications links, while generally static, are at least multiple and of a diverse nature, to provide a degree of flexibility.

B. Problems

I hope I do not mislead anyone into thinking that a solution to emergency communications problems is available with the advent of computed networks. The economic environment for communications technology is rigorous and risky; there are complex regulatory issues dealing with interconnection of common carriers, direct broadcast satellites, and the deregulatory vice competitive aspects of radio and common carrier communications, to name just a few. I do not mean to imply that the horizons are unlimited; but there is significant communications capability potentially available which has not been exploited for emergency communications.

Similarly, anyone who has ever dealt with a retail company to correct an error in a computerized bill knows the foibles of depending on computers. Let me cite a few of the problems that the military and the intelligence communities have had to deal with in the area of interconnecting of computers. I understand that the subcommittee will be hearing more of these matters later in these hearings and so I will be brief.

What are some of the realities in working with interconnected computers? An important problem is one that deals with language. The man-machine interface is bridged by a language that the computer must understand. The man must be flexible enough to re-interpret his needs and his questions into computer-compatible language. Senior decisionmakers usually do

not work with such languages directly and therefore must have "interpreters", or programmer/analysts, generally a hierarchy of them, to assist him. Thus, needs may be reinterpreted variably and misunderstandings and errors can creep in to the process. Such an information network may well develop a flaw, in that the decisionmaker's needs are redefined to fit the information system's capabilities instead of the other way around.

Another problem is what I call the "embarrassment of riches" problem. With multiple sources of information and with sources which individually generate a plethora of data, it is quite easy to flood a decisionmaker with a mass of raw, undigested, redundant, incorrect, or outdated information, leaving it up to the decisionmaker to select what he needs. When this happens, and it does happen, the very natural response of the decisionmaker is to ignore all the data; there is just too much chaff for such a small number of kernels.

Yet another problem is the situation in which all users of the information network are not equal and can have only limited access either to data or to selected nodes, even though there is a physical capability for access. In the military or the intelligence area this is manifest in the hierarchy of classification of information; in the domestic area, the corresponding concept is that of privacy and confidentiality of information. To exclude access to those with the physical capability for interconnection, but with no legitimate need for access, is a difficult problem.

While not wanting to throw cold-water on information networks, the "realities" of dealing with computers (frequently indirectly) should be acknowledged. I have mentioned only a few of the problems. But what is the potential for information networks?

C. Potential

Dennis

Despite the manifest problems, the potential for information networks is difficult to overestimate. The flexibility that they apparently have to deal with a variety of crisis situations is the reason that they can and will be very important to emergency management and to national defense. Emergency communications must be less vulnerable to the disorganization wrought by crisis or disaster in order to be able to deal with these situations effectively. Information networks appear to have the potential to improve this situation--not only in their increased survivability, but also in their ability to provide capabilities when trying to ascertain the facts in an emergency such as feedback, cueing sensors for additional or more detailed data, or permitting a query-response-requery cycle.]

Let me digress a moment to develop an analogy for information networks. Norbert Wiener was a brilliant and distinguished professor at the Massachusetts Institute of Technology who is credited with founding the science of cybernetics--automation or control. Professor Wiener had noted that there were common principles in a human being's central nervous system (with its sensors, its nerve paths, and its brain) and in the workings of a computer (with its data bases or sources, its links, and its central processing units). Both entities function similarly to respond to their environment, i.e., to deal with their problems and to survive. Let me extend this idea to the view of the nation as a whole, which under stress relies on its "information networks" and the internetting of these networks to function in a crisis to help bring order out of the disorder of a crisis--with the ultimate goal of survival. That is what drives the human machine. And that is what should be driving the national effort in emergency management by means of its information network(s).

Are these musing far-fetched and practically speaking not really very

useful? I hope not. Citizen band radios had been around for quite a while before a fuel crisis threatening severe economic problems helped to increase the public awareness of CB's and of their utility. The private radio services of the country, the common carrier and cable facilities, and broadcast equipment all constitute our national telecommunications resources--our information networks. Let us also keep in mind that computers eventually are likely to become necessary and inexpensive household appliances. [The day may not be too far away when "intelligent", i.e., computer-assisted, processing of vital information via dynamic communications, allow a remote and isolated decisionmaker to bring order to a range of crises--domestic crises, state-wide catastrophes, or nation-wide emergencies. The technology is coming along rapidly and I am optimistic that emergency management can exploit these rapidly advancing communications technologies.]

I would be happy to elaborate on any of these points or to answer any questions.

Mr. GORE. Thank you very much. I do not know when I have been more impressed with testimony. I really appreciate the amount of time and effort you obviously put into that. Thank you very, very much.

What about this conflict between competition and the goals of computer users and the survivability and viability of the emergency communications system?

Mr. LUKASIK. Well, I think that this is basically a political question that the Congress will have a major voice in deciding. There is in the Senate, of course, 898, which is the Communications Act rewrite, the current Communications Act rewrite that deals with a number of the questions, A.T. & T.'s structuring of the relationship of national security needs and how they are provided for in the Communications Act. You are, of course, familiar with Mr. Wirth's House Communications Subcommittee, the oversight committee for the FCC where these same matters are dealt with.

The Communications Act under which we operate mandates the lowest possible cost, and that translates in not only the current policies but the policies that have been pursued by the Commission for a number of years into encouraging competition.

I think the key issue here is what are your expectations for innovation and what is the best way to encourage it? There is no question that the Bell Telephone Laboratories is a superb organization and has given rise for many decades to major, major advances in the science of communication, but that organization is not the only source of innovation in our country. It is not responsible for the major growth in the computer industry, and that is what is essentially driving the new information technologies and having major impact on the way communications systems are used to provide information to people.

So I have no ready and easy answer. We have gotten to where we are as a result of competition, and we now are facing the difficult problem of how to balance the desirable effects of competition both from the standpoint of innovation and from the standpoint of providing communications services to the people in this country at the lowest possible cost, which is mandated by the Communications Act, with the necessity of maintaining some kind of system coherence. Coherence in the planning of our investments in communications facilities, coherence in the management of those facilities in the most efficient way, and, of course, under the circumstances that the—that several of the previous speakers have addressed, that is what do you do in the case of the utter disaster of nuclear conflict where clearly the greater degree of centralization provides important management advantages.

I think that what the political decision must be faced with, is how much of the protection, how much of the cost of the protection that clearly must be built into our communications systems? I think there is absolutely no question on that score. How will these improvements and enhancements be funded? Will they be funded by the communications ratepayer, or will they be funded by congressionally appropriated funds for defense and emergency preparedness? That is, I think, the central issue that—on which the Congress must speak and must speak clearly if the threats that we face are to be met and if the technological capabilities that are available to us are to be built into that communications system.

Mr. GORE. If you quantified the amount of money spent for the purpose of anticipating and coping with emergency management crisis situations spent on the landlines and microwave systems, what would the magnitude of that be? Hundreds of millions per year?

Mr. LUKASIK. That is a very difficult question to answer, Mr. Chairman.

I, quite frankly, am not a common carrier accountant, and I would not want to give numbers off the top of my head. I will certainly have them supplied for the record.

A.T. & T., that constitutes about 80 percent of the common carrier business, domestic common carrier business, is—has annual revenues of \$40 billion, of course. Their capital equipment expenditures are in the billions. Now how much of that goes for the protection of the system? Very little explicit funds go into the protection of the system. There is, of course, the question of dispersal of facilities, hardening of facilities, of EMP protection. Those have been mentioned already. Those numbers, I am sure, can be found or at least—what is more important, you can find the cumulative costs over the last 10 or 20 years.

But in the design and planning of the system for purely commercial purposes, you do many things that also assist in the enhancement of that system for the provision of emergency services. You obviously have to build spare capacity, because you cannot run out of capacity. The leadtime in installing equipment is often 3 to 5 years and more, so, therefore, you always have a lot of equipment installed in anticipation of needs that must be met before new equipment can be installed. You also have the simple procurement and installation cycle.

Mr. GORE. Yes.

Mr. LUKASIK. They want to build redundant systems. They want to build systems whereby traffic can be rerouted for the very simple reason that there are large amounts of calls placed on Christmas, Mother's Day, and so on that have to be accommodated also.

So the growth in the system, it is not easy to pin down the number of how much goes for protection for national disasters and emergencies. The point was made earlier about fiber optics. Fiber optics is relatively immune to EMP, although there is obviously a lot of terminal and switching equipment that is not immune to EMP; nevertheless, the basic lines are less immune to EMP. They are smaller, so they can be easily buried, and that provides a great deal of protection; and the common carriers are going to fiber optics for the very simple reason that they have satisfied themselves that it is cheaper than copper. The repeaters can be spaced more widely apart, and that is a major part of the system, because the optical fiber cable has less loss than microwaves and the like.

So to really get at what you are after, and it is an interesting and important question, is not an easy one. It is not to be found in explicit line items in the budget, although there will be some of those. But it is instead to be found in what are the normal practices by which a network is planned and constructed and maintained.

Mr. GORE. Just another one of those vexing joint cost allocation dilemmas. There is a document in the Justice Department's anti-trust case against A.T. & T., which estimates the cost at hundreds of millions of dollars per year that are presently added to the telephone rate base; and as we move further down the road in the competitive era, at some point the cost of emergency communications systems, both for military and civilian purposes, probably are going to have to be separated from the rate base in order to equalize the competitive postures of the dominant carriers and the others.

Mr. LUKASIK. I think that is right. Certainly some way will have to be found. One cannot have unequal treatment of all carriers, and the fact that one is a monopoly carrier does not mean that that carrier is to be treated unfairly, either. Clearly there has to be an enhancement not only in the A.T. & T. system but in the additional communications facilities that these other carriers are constructing. So it is a question that is clearly becoming more important as the years go by and one for which an—both a political and an economic solution will have to be found.

Mr. GORE. Well, thank you again for spending so much time in making this testimony as good as it is.

We are going to have our second day of hearings tomorrow morning at 9 a.m. in this same room. With thanks to all of the witnesses who appeared today, we will adjourn at this point until tomorrow morning.

[Whereupon, at 12:55 p.m., the subcommittee was adjourned, to reconvene at 9 a.m., September 30, 1981.]

EMERGENCY MANAGEMENT INFORMATION AND TECHNOLOGY

WEDNESDAY, SEPTEMBER 30, 1981

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
Washington, D.C.

The subcommittee met, pursuant to adjournment, at 9 a.m., in room 2318, Rayburn House Office Building, Hon. Albert Gore, Jr. (chairman of the subcommittee) presiding.

Mr. GORE. The subcommittee will come to order. I would like to welcome all of our guests.

This is the second day of this subcommittee's inquiry into the Nation's emergency preparedness. Yesterday, we heard from a group of distinguished witnesses about the importance of secure and rapid communications that could convey information in the event of emergencies to decisionmakers in a usable way.

We heard about marvelous advances in communications technology that are light-years ahead of the actual technology that is now being used. And we heard about an agency, FEMA, that is just now beginning to pick itself up off the floor and make its weight known in the Federal establishment.

It was a fascinating trip into the world of contingencies, redundancy, and photonics. It was also a disquieting trip because of the distinct impression conveyed by all the witnesses that we are really not where we should be.

Today, we want to turn our attention to a subject that complements those we spoke about yesterday. It is important that we look more specifically at the various kinds of networking involved in dealing with emergency situations, including both the human interactions involved and the different kinds of support that are now possible by using technologies ranging from telephones and teletypes to satellites and multipurpose computer configurations. One of the largest problems in the whole area is our current inability to match the possibilities of the technology and the limitations of the people who must use the technology. It will be important to see how we can modify the technology to make the man-machine interface a good one.

I want to emphasize again today the bipartisan nature of this effort, and the continuing nature of our activities. I am convinced that the only way that FEMA and other civilian authorities will get the clout that they need is through vigorous congressional oversight. Only through the continuous application of pressure from all sides will we get both the human and the technological

commitment to deal with the critical problems in managing the effects of disasters.

I would like to recognize now my colleague, the ranking minority member, Mr. Walker.

Mr. WALKER. Mr. Chairman, yesterday we heard from a number of witnesses who painted an interesting picture of our ability to respond to crisis. Technology continues to rush forward at a pace which far exceeds man's abilities to adequately utilize the progress achieved.

We heard of progress which belies the imagination in the manner in which information can be transmitted and received. We are all familiar with the advances in the field of computer technology. Now we are told that we can handle, transmit, receive and manipulate data at a speed of millions of characters a second. It is too bad that man himself can only comprehend that same data at a speed of about 40 characters a second. As that great social philosopher Pogo used to say—"We have met the enemy and he is us."

The ability of Government to respond to crisis may easily make the difference between tragedy averted and major loss of life. The possibilities are endless. Fire and flood annually take hundreds of American lives. Tornadoes and hurricanes periodically ravage our land. And after the accident at Three Mile Island we now must realize that nuclear accidents are well within the realm of probability. Recent events around the world should also have taught us that no land is immune from terrorist activities.

We hope that the result of these hearings will be a better understanding of the problems of handling information and communicating in emergency situations. We also hope that the result will include an increased ability of our Government to respond rapidly and effectively to crisis.

In my own area of Pennsylvania we have had to survive two major disasters in recent years. The first was Hurricane Agnes. That storm brought widespread flooding and heavy damage to most of Pennsylvania. The response of the Federal Government was adequate, but somewhat slow. The response to Three Mile Island left much to be desired.

In the first days after TMI, there were no less than three different Federal agencies which felt that they were the lead agency. Each gave orders—which were often in conflict with each other—and efforts were hindered in the process. We discovered that the various agencies did not know what the others had in their computer data bases—and what was worse, the computers could not talk to one another. The result was that it took far longer than was necessary to develop an effective response to a problem of major proportion. That long period of time was not satisfactory—and could have been deadly had the problem at TMI been more serious than it actually was.

We hope that by bringing these problems to light, we will be able to stimulate progress in this important area. I would like to point out again that this is a bipartisan effort within this committee, and I congratulate my chairman for his interest, and it is also a joint effort with the Reagan administration. I trust that our efforts will be productive.

Mr. GORE. Our first witness is Dr. Thomas G. Belden, a consultant working now at Rockville, Md. He has been an analyst with SRA, SRI, with the Institute for Defense Analysis, working with the Assistant Chief of Staff at the Air Force and with a number of other assignments.

I guess he is best known to some for an analysis of the major crises in emergencies like the Pueblo incident, Pearl Harbor, and others, and we are pleased to have him help us on this occasion.

Dr. Belden, if you will join us at the witness table.

Without objection, your statement will be included in the record in full and we invite you to proceed with the presentation of your statement, a summary or all of it, as you see fit.

**STATEMENT OF THOMAS G. BELDEN, CONSULTANT,
ROCKVILLE, MD.**

Dr. BELDEN. Thank you, Mr. Chairman. I am deeply honored to be here. I recently retired from the Government, and I really appear before you just as a private citizen. Even my clearances are not extant any more. Half the time I don't know that I am authorized to hear what I have to say.

I, also, wish to apologize because of a failure in communication on my part, in that I don't have a written statement ready for you, because I came here on very short notice. It wasn't because Mr. Chartrand had not made valiant efforts to get hold of me, as long as 3 weeks ago, but I was living on a little remote island on northern Lake Huron, and I have no telephone.

Mr. GORE. You don't know anything the rest of us should, do you?

Mr. BELDEN. So I have submitted to the committee an article that I had written some time back. Perhaps its only virtue is that it has been cleared by the CIA, but it does contain a great many of the viewpoints that I will be showing here.

I was absolutely fascinated by yesterday's testimony of all the witnesses. I thought they were excellent. I share the problem, however, that you have, that you brought up in your introductory remarks, and that is, with all the marvelous technology great things that can be done. Technology, as you know, is double-edged; it creates problems, and I would like to address some of the problems created by technology.

First of all, there is always a tendency to build systems where man becomes the servant of the machine rather than the other way about. The focus should be on the human being because that is the heart of the matter. Most breakdowns are not hardware breakdowns but human failures according to the postmortems that I have done. Unfortunately, I won't have time today to go into any of those postmortems; there just simply isn't time, but I would like to make that point.

We are putting out more and more data at faster and faster rates, and they have to terminate ultimately in something called a poor human being. He has a very limited bits rate; he is good at recognizing patterns, but information is not presented tomorrow in such a way as to enhance that capability.

Also, as we build more channels of communication, they tend to become filled, and that increases the volume, and as you increase

the volume of information, the probability of being able to select that which is relevant goes down. In other words, we are being submerged by information beyond man's capacity to handle it particularly because the way it is presented to him.

Mr. GORE. Doctor, if I could interrupt, I think that might better be referred to as ex-information. It is of no use to us, and it is accumulating in such vast quantities, almost in direct proportion to the contrast between the 40 bits per second and the billion bits per second or trillion bits per second in the photonics referred to earlier.

It is a problem not only in the emergency management area but for our civilization generally.

Mr. BELDEN. I totally agree with that.

Also, I might point out that the marvelous systems that we have—for instance, the one that Dr. Baker described—the Bell network, and he showed a viewgraph about that—that is superb. However, I am haunted by the possibility that someone, say, a terrorist who is rather smart, can use our systems against us. It is a kind of social judo.

In other words, with the advance of plastics and explosives, the ability to hide them at certain critical junction points, nothing as dramatic as a powerhouse, but just the unguarded power nodes, he can connect it into the Bell System and use long-distance dialing from another country to detonate it remotely. If he did it in the right places—you heard about the manhole in New York, and so forth—this makes us extremely vulnerable. It is using our Nation's strength against us, as in judo.

Now, I could go on with other examples, but I would like to get on with some other factors.

The postmortems of crisis always reveal how much information was in the system that was never used that was critical and vital. This is a very large problem because of this volume of data problem, and this lack of ability to retrieve and converge that which is relevant.

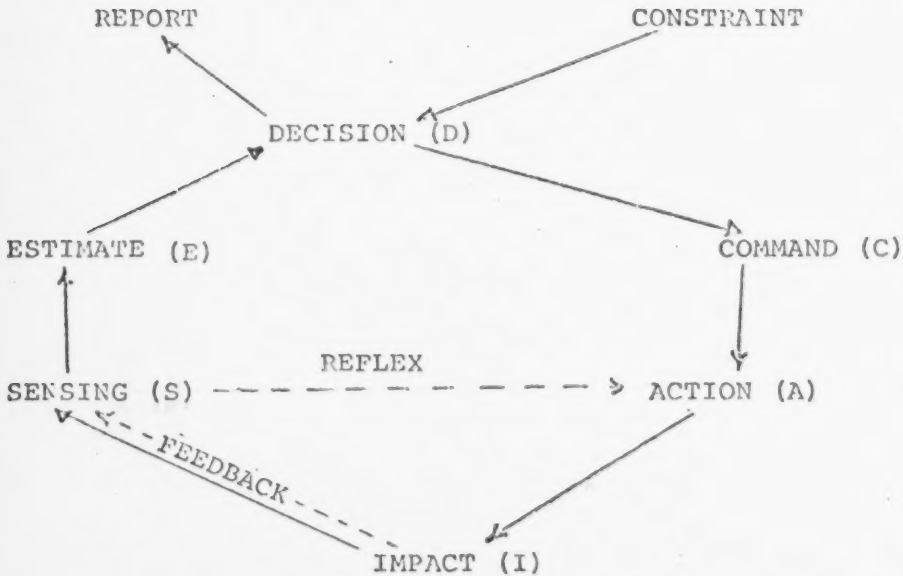
I am sorry I am going to bring up more problems than I am solutions, but I wanted to bring it to the committee's attention.

Now, I think that, as I said before, the human being is the heart of the matter. Most people come in with models of systems or mechanistic models. The model I am going to be using is the human being, himself. We all practice command control in our lives every day.

[The chart, "The Decision Hexagon," follows:]

Figure 1

The Decision Hexagon



Mr. BELDEN. Now, when we operate as human beings, we go through a process like this. There are other ways you can put it, other words you can use, but I think you will catch what I am going to say. For instance, I sense that I see somebody smoking and that makes me want to smoke my pipe. So I do an estimate. Do I want to take another chance with cancer, and so forth, and I say, yes, but then I have to give myself some other inputs. I look around to see if there are any no-smoking signs. Do I have to tell anybody I am going to smoke my pipe? Well, I finally satisfy all this, and I make a decision to smoke my pipe. Now, I have to give myself a series of commands to get out my tobacco and my pipe, and then I take the action of lighting my pipe.

The action results in my burning my finger with my lighter, and I take a reflex action and store that in my memory and say, "Don't do that that way, you idiot; you are going to burn yourself."

I go through sometimes the complete loop of this decision process. Other times, I have reflex actions or I have preset decisions, and so on.

That is what we do in our lives when we drive a car or anything else.

When the problem becomes larger than what one human being can handle, we tend to divide this among people, say, a staff. Over here, this tends to be the intelligence, or J-2 side in the military. This is the J-5. Going down here is the operations, or J-3. This is

planning. This is operations. They are in charge of giving commands, and so forth, to take the action.

So we even organize ourselves around this basic human decision loop and, of course, all of these lines connecting one to the other is some kind of communication, either face to face, or telephone, teletype—whatever.

Now, we hear a lot about the national command authority. In the hexagon that is the downside or command side. Everybody can define that quite distinctly, from the President to the Secretary of Defense, through the JC's, the unified, specified command for component forces, or any other part of the Government, for that matter. These are well defined.

Where the problem is is the upside—the control side. Who can define what that looks like?

There are many, many organizations, and lots of confusion.

One of the reasons for this is every crisis is unique and different parts of the Government have to become involved, and you don't know that until you are into the crisis or have had warning about it.

Therefore, it is very difficult to define the upside of this crisis decision process. This creates all kinds of problems of trying to define who is in charge of this particular aspect of the crisis.

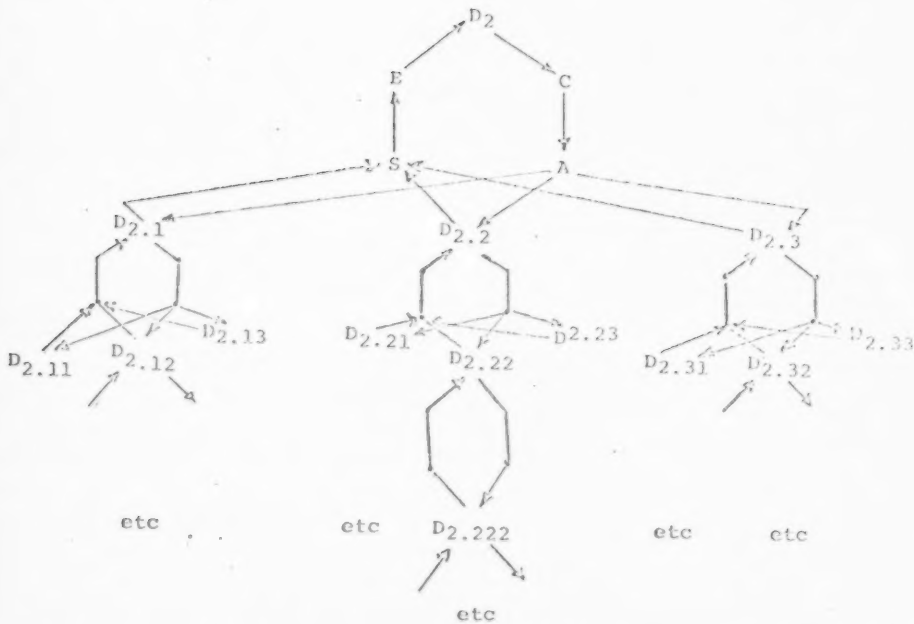
I will go into that a little bit more later, but that is the first dilemma.

We cannot define the organization until we are in the crisis in order to get to the substantive people who should handle it.

[Chart entitled "The Hierarchy of Decision Hexagons" follows:]

Figure 2

THE HIERARCHY OF DECISION HEXAGONS



Mr. BELDEN. In the hexagon I showed before, actually there are thousands of hexagons in the Government. They are in great pyramids of chains of command from the President to a destroyer in Southeast Asia. There are 11 different possible decision points in that chain of command.

Now, in a crisis, this creates a second dilemma, and that is, obviously you cannot go through that whole command chain during a crisis. There simply isn't enough time to go up and down the command chains, and this gives rise to the issue of centralized versus decentralized command and control. That complicates things because our communications systems are basically built on this basis in the decentralized mode, and it is very difficult for them to shift gears during a crisis into a highly centralized mode.

They argue back and forth as to whether you should have centralized or decentralized command and control. I think the argument is pernicious. You have to have both. The art is to know when to use which.

[Chart entitled "The Warning Process" follows:]

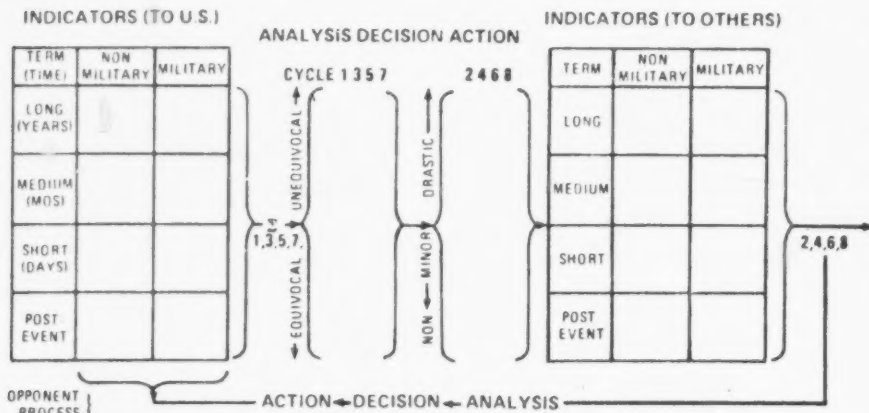


Figure 1: The Warning Process

Mr. BELDEN. The next problem that is terribly confusing in all kinds of crises is the definition of this word "warning." Everybody has a different definition. It is only fair to tell you mine. To me, warning is not warning unless decisions and actions are implied. In other words, warning to do what? If we hear on the radio this morning here in Washington that tornadoes are going to hit Topeka, Kans., at 3 o'clock this afternoon, to us here in Washington that is a forecast. If you live in Topeka, Kans., it is a warning, because it implies you have to make some decisions to take action.

If you look at warning from that point of view, then the warning process looks something like this.

First, you have indicators. They can be military or nonmilitary—that is, all other parts of the Government, political, diplomatic, domestic, civil defense, what-not. They can be long-term, mid-term, short-term, and they even include the events after the egg hits the fan.

Now, the problem in the intelligence world is to converge all of these indicators to make some kind of an analysis. The analysis we make leads to a decision. The decision we take leads to some kind of action. The action we take, wittingly or unwittingly, becomes a potential indicator to the opponent, and he does the very same thing we do. He converges his indicators; he makes an analysis to make a decision, to take an action, and his action becomes a potential indicator to us; and so the cycle becomes complete.

Some of these cycles are years long, in the case of the development of a new weapons system, or they can be months long, days long, hours long.

The point I am trying to make is that in crises that do not involve natural phenomena, such as an earthquake or hurricane; that is, in crises that involve the interaction between two parties, the decisions we take affect what he does, and what he does affects what we do. Very often this is neglected in plans and operations and in intelligence assessment.

As I will try to explain later, it is very difficult sometimes even for our own intelligence to know what our own operations are so

that our intelligence organizations can look at the right place at the right time at enemy responses in order that we can take the proper action. I will dwell on that a little bit later.

Another thing I would like to emphasize here is in this decision process, this interactive process, it goes by a series of steps. If the opponent is at all rational—this can be a nation, or it can be a terrorist group, or whatever—he must go through a series of decisions.

[Chart entitled "Decision Stairway" follows:]

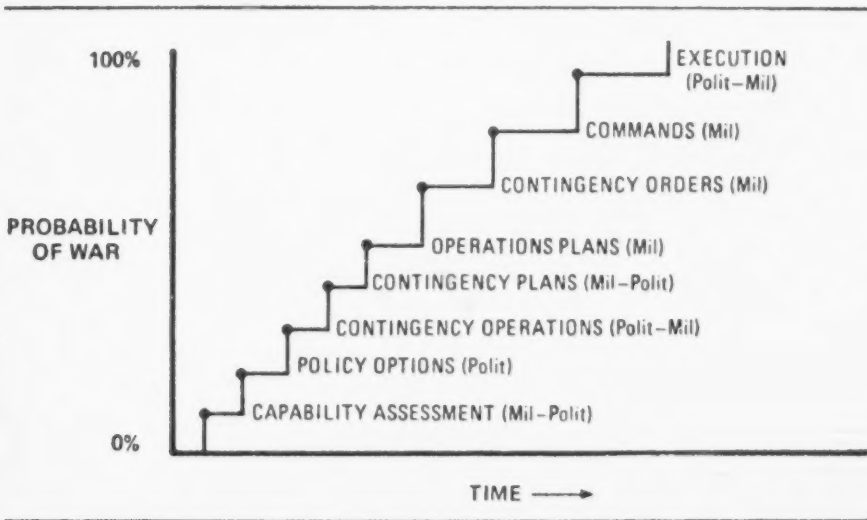


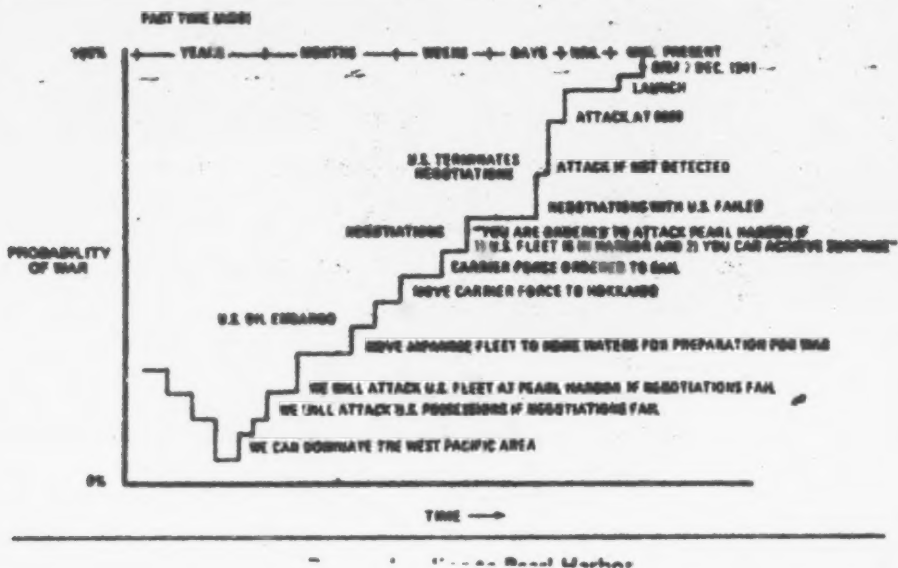
Figure 2: Decision Stairway

Mr. BELDEN. The horizontal axis here is time. The vertical axis is the probability of war. The point is, he starts out with a high probability of no war, and, as he goes up this stairway, the probability of war is increasing. In other words, he first has to figure out what he can do, and as he gets irritated, he considers what are his policy options. As he gets more irritated, he considers his contingency options, and they get more military; and finally, you get up here to the command of execution.

The important thing is at any point in this process the opponent can change his mind and go back down the stairway, either for his own reasons or because of something you did, wittingly or unwittingly.

Maybe I can be a little more concrete to illustrate this in the Pearl Harbor case.

[Chart entitled "Japanese Decision Process Leading to Pearl Harbor" follows:]



Mr. BELDEN. Here is the same stairway. As you go up, you increase the probability of war. This all takes place over time on the horizontal axis.

In the late 1930's, the Japanese built up their capability to the point that they could dominate the Western Pacific. In the meantime, they had gone to war with China. That irritated us with them; we began to impose certain economic sanctions against Japan. That irritated them. Finally, we at this point imposed the U.S. oil embargo on Japan. That has a faint echo these days.

At that point, the Japanese decided to make the detailed plans to attack Pearl Harbor. Now, the Japanese are still 18 months away from that event, but that is when they started to plan it.

In the meantime, we were negotiating with the Japanese. The negotiations were getting nowhere. Finally, Admiral Nagumo, the commander of the Japanese carrier task force, was ordered to sail from home waters in Japan and start across the Northern Pacific.

When he opened his sealed envelope the second day at sea, it told him, "You are to attack Pearl Harbor if two contingencies are satisfied: First, that the fleet is in, and, second, you can achieve surprise."

Now, Admiral Nagumo is going to get the intelligence from a small but effective Japanese intelligence group in Honolulu to tell him the condition of the target. He is also told in his orders that if he were only 1 day's sailing away from his launch point off Oahu, that if he were detected by the U.S. fleet, he was to virtually go up on deck and bow and say, "We are only here on an exercise," and take the Japanese fleet back to home waters. Those were his orders.

It is interesting to surmise if we had a warning system sufficiently alert to be able to detect the fact that he was on his way and also had we been sophisticated enough to let the Japanese know that we knew, then Nagumo would have followed his orders and

BEST COPY AVAILABLE

taken the fleet back to Japan. In a case like this, warning and crisis operations can become a deterrent.

The interesting thing is, in order to make a prediction about what is going to happen, you have to put it in probabilistic terms because the prediction isn't necessarily going to come true because the opponent can change his mind by something that you do in the meanwhile.

It is terribly difficult to predict another person's actions when that other person hasn't made up his own mind what he is going to do yet.

I guess what I am trying to say is: I am ruining the James Bond or romantic school of intelligence where the secret agent comes in 3 weeks ahead of time and gives you a message to say Pearl Harbor is going to be attacked at 8 a.m. on December 7. No way. They haven't made up their minds whether they are going to attack. And a good decisionmaker will keep this stairway up as high as he can as long as he can. It is called keeping your options open. This is what makes predictive intelligence extremely difficult, and it requires that any intelligence estimate be put in probabilistic terms and the consumer of intelligence has to accept that.

Now, to make such a stairway, it takes all kinds of intelligence. Not just military intelligence, but domestic intelligence, political, diplomatic, economic, all of it. And that means that it has to be collected from a wide variety of agencies in the intelligence community.

Let us take a look at the intelligence community since Pearl Harbor.

[Chart entitled "Intelligence Organizations, 1940-1951" follows:]

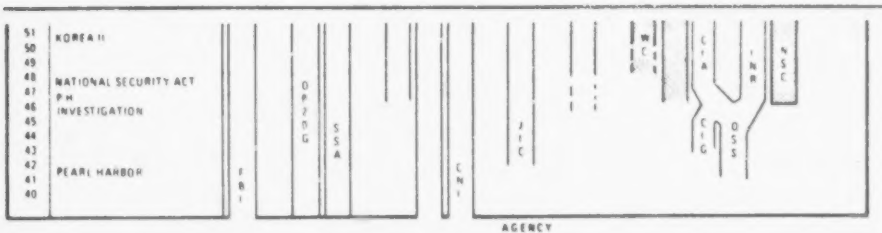


Figure 8a: Intelligence Organizations, 1940-1951

Mr. BELDEN. At the time of Pearl Harbor there were but three intelligence agencies, the FBI, the Army's G-2, and the Office of Naval Intelligence.

Here is the way it looked after Korea. New things are growing in the intelligence community. Time marches on.

[Chart entitled "Intelligence Organizations 1940-1969" follows:]

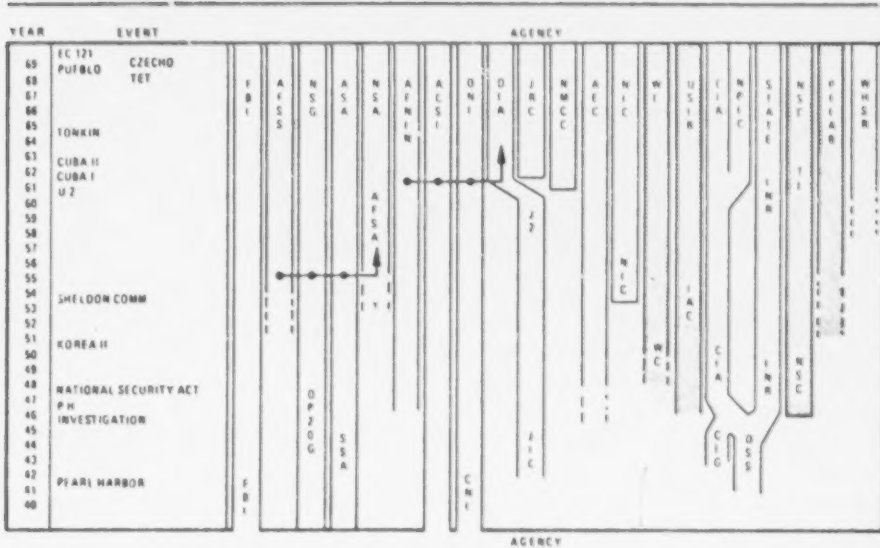


Figure 8b: Intelligence Organizations, 1940-1969

Mr. BELDEN. Here is the way the community looked 10 years ago. Now, I am not being critical of any of these agencies. They all do excellent work. The problem is, as you increase the number of agencies involved, the ability to converge the relevant critical information goes down. It is bound to. This is a real problem. I haven't drawn the current chart. First, I don't know if I could any more. Second, I would like to keep my sanity for one more year.

But there is the problem—how do you connect and converge information across all of these agencies?

Well, in early 1973, the Air Force loaned me to the intelligence community staff. No one knows what that is, I don't suppose. It is a group that works for the DCI. It is not part of the CIA, or at least wasn't at that time. Its objective was to try to pull the community together. I think it has since disappeared. It disappeared in October 1978, but that is another story.

Now, when I was loaned to the agency, I had an objective. First, you know the panacea of all Government ills is to either reorganize or create a new organization. When I went out there, sure enough, they were reorganizing.

I made a plea: Don't reorganize; use the organization as it exists, but give it some communication laterally that it has never had before. Because if you lay out crises in terms of the amount of time you have to deal with them, like a very short crisis is the shoot-down of EC-121, the Cuba missile crisis is days long. The energy crisis is a creeping crisis that goes over years.

There is lots of organization for the longer types of crises. Where the gaps seem to be is for the shorter ones.

Instead of filling that gap with a great bureaucratic structure, my recommendation was to put in some conference communication networks.

The first one we put in was called the NOIWON, the National Operations and Intelligence Watch Officers Net. Now what this did was to connect the watch centers, the 24-hour watch centers, by secure conference telephone, and these centers with the CIA, the NSA's, NSOC, DIA's, NMIC, the J-3's NMCC, the State Department's operations center, and State's intelligence research department and the White House situation room.

In other words, there were seven 24-hour centers that we wired together by this secure conferencing voice system.

Initially, it only cost \$50 to put this together. It only took 2 weeks to make it technically functional, but it took me 10 months to make it operational, because of the cultural differences among the players. CIA types did not like to talk to J-3 types, et cetera, et cetera. It took the trauma of the *Mayaguez* incident to get this done. Government learns by traumatic experience. Now NOIWON is part of the woodwork. They use it all the time and don't think about it. Resistance has collapsed.

I also tried to put in another system at the analytical level which allowed them to do the same thing. It was a slightly more elaborate system that allowed word processing computers to be located at five places around Washington, the Pentagon, State Department, NSA, CIA, and it also connected them with a secure-voice conferencing capability, so they could conference from room to room at each remote location. This system has been in existence for over 3 years. It was in existence since early 1978. It was used very successfully on one occasion when they asked me to set up a conference. I got all kinds of kudos and letters how great it was, and, to my knowledge, it has never been used since.

The reason for this is bureaucratic. It is very dangerous for an analyst to commit himself across the community in this fashion. They will do it under crisis situations where the urgency is so great, but what we have here is a human problem, not one of technology.

Now, the first objective of warning and crisis operations, of course, is crisis avoidance. Don't have a crisis unless you have to. If you can't avoid the crisis, keep it political. If you can't keep it political, keep it limited-military. If you can't keep it limited-military, keep it limited-nuclear and gracefully degrade to Armageddon. But to do this takes a very sensitive national nervous system in order to be able to control the situation and get the relevant information that you need at the right time.

Now, we have put an awful lot of money into retrieving data. We have put very little into retrieving people.

Every time there is a crisis which is unique, you scurry around really to find who is smart about this, substantively smart people. Not necessarily the high levels. And how do you put them together? How do you wire them together?

To me, this is a great lack in our current system. It is not so much technology; it is a human problem, a bureaucratic problem, and also there are many other problems here, and that is, how do you preserve dissenting views in such a system? How do you guard

against misinformation, disinformation. Most people assume that all the information and data is correct. It isn't necessarily true. It is only human judgment that can be involved here that will detect misinformation.

I will close by quoting James Thurber, one of his fables for our time, "Get it right or leave it alone; the conclusion you jump to might be your own."

Thank you.

[The prepared statement of Mr. Belden follows:]

Statement by Dr. Thomas G. Belden

Indications, Warning, and Crisis Operations

THOMAS G. BELDEN
*Intelligence Community Staff
Washington, D.C.*

Since the warning process goes beyond the sphere of intelligence to impact on decision-making and action, warning and crisis operations have broader objectives than is often thought. The warning process—whose primary elements are indicators, analysis, decision, and action—is conceptualized in interaction terms and further specified using the notion of actor's decision stairways. An objective of any intelligence and warning system is to determine the opponent's position on the decision stairway toward action. Pearl Harbor and the Yom Kippur War illustrate the interaction of participant's decision stairways. Innovations in communications and conferencing techniques, designed to mitigate organizational problems in warning and crisis operations, are described. Suggestions are offered for improved use of probability statements by analysts.

The primary objective of state-conducted intelligence is to acquire information which contributes to warning. However, the warning process goes beyond the sphere of intelligence to impact on the area of decisions and actions. Consequently, warning and crisis operations have a broader series of objectives than often is thought to be the case. These are:

- (1) Avoid or head-off a potential crisis situation (crisis avoidance).
- (2) If (1) fails, manage the crisis so as to satisfy national policy objectives without resorting to military force.

AUTHOR'S NOTE: The ideas contained in this article are those of the author and do not necessarily represent those of the Intelligence Community Staff or any other official agency of the U.S. Government.

INTERNATIONAL STUDIES QUARTERLY, Vol. 21 No. 1, March 1977
© 1977 I.S.A.

[181]

BEST COPY AVAILABLE

[182] INTERNATIONAL STUDIES QUARTERLY

- (3) If (2) fails, use conventional military force and diplomatic efforts to avoid long or severe conflict, conventional or nuclear.
- (4) If (3) fails, end the conflict on terms as favorable to our interests as possible before Armageddon.

Although the above steps appear to be obvious, it is not clear that our national "nervous system" is designed for the interactions which must take place among our bureaucracies in order to operate effectively in crisis warning situations.

The Director of Central Intelligence (DCI), the primary foreign intelligence advisor to the President, is deeply involved in the organizational issues raised in warning and crisis operations. One of the principal functions of the Intelligence Community Staff (of which the author is a member) is to assist the DCI. Over the past three years, we have designed and developed certain communication facilities, techniques, and procedures, some of which are operational while others are still in the developmental stage. Many of these are discussed in this article, including the development and use of "decision stairways," "Meet-Me-Bridge" teleconferencing systems, and probabilistic statements regarding the likelihood of potential crisis. The communication procedures discussed below were developed in response to the tremendous informational burden placed upon the crisis forecaster and manager and the lack of organizational progress which has been made in the area.¹

The Warning Process

"The warning process" is one of the most misunderstood concepts in national policy analysis. The terms "indicators," "intentions," "capabilities," and "estimates" are also used in a wide variety of ways. The problem is continually exacerbated since the term *warning* itself is tied to many other vague words (e.g., strategic warning, tactical warning, political warning, military warning, warning indicators, warning time, long-term warning, and short-term warning).

Warning has one characteristic that separates it from estimates or forecasts: it implies decisions to take actions. For example, to residents of Washington, D.C., a radio bulletin that tornadoes are going to strike Topeka within the next four hours is an estimate or forecast. However, to

1. For a different and more detailed perspective on communication and conflict decision-making, see Haas (1974: 98-122).

residents of Topeka, this same information is a warning because it implies that they should make decisions to take protective action.

The warning process is described in Figure 1. On the left is a matrix of indicators (long-term down to short-term and military versus nonmilitary). The indicators are generated by the opponent's activity. The convergence and summation of the indicators leads to an ANALYSIS that, in turn, leads to a DECISION to take an ACTION. The ACTION generates indicators to the opponent, who goes through the same type of process: ANALYSIS-DECISION-ACTION. (See bottom of Figure 1.) His ACTION in turn becomes an indicator to us, completing the first cycle. The cycles are repeated in a process of action and response. Some of the cycles take years to complete; others, only hours or minutes. As events draw close to the hour of action, the action-reaction cycle becomes extremely complex and often unclear. Even in hindsight, the cause-and-effect relationship of particular responses to particular actions often becomes indecipherable.²

In the middle of the figure, ANALYSIS is evaluated on a vertical scale, ranging from equivocal to unequivocal. ACTION is also on a vertical scale, running from non or minor action to drastic. Although sometimes

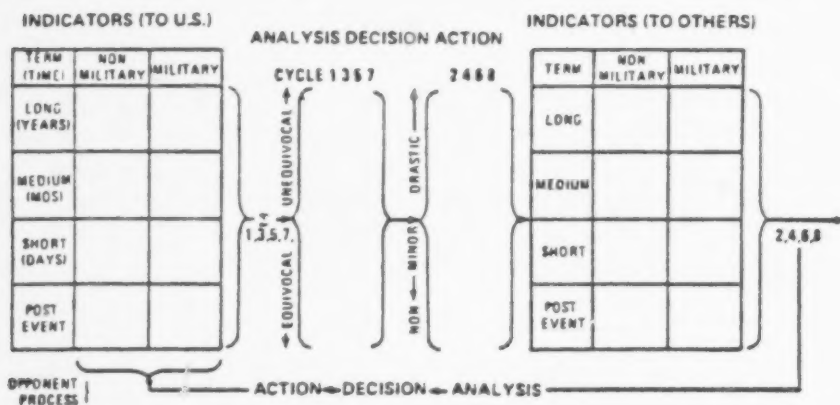


Figure 1: The Warning Process

2. Although there are superficial similarities between this model of the warning process and the mediated stimulus-response model of the Stanford group, there are several important differences, e.g., the latter put much more emphasis on perception than does the former. See, for example, Holsti et al. (1969).

[184] INTERNATIONAL STUDIES QUARTERLY

necessary, it is risky to take drastic action on the basis of highly equivocal indicators. However, it is possible to take less than drastic action, such as going on alert, on the basis of equivocal indicators, e.g., a 40% chance that a drastic event will occur. This topic will be discussed in more depth below.

Depending on one's objectives, there are many possible strategies for interaction. On the one hand, the opponent's decision can be made more difficult by increasing the ambiguity, or equivocality, of indicators sent to him. On the other hand, if one wants to prevent the opponent from taking drastic action, it might be desirable to communicate intent as clearly as possible.³

Unfortunately, our government is not organized to meet the demands of the warning process. There are some major bureaucratic barriers not shown in Figure 1, particularly between the ANALYSIS and DECISION functions (the intelligence community and the policy and decision makers) and between the ANALYSIS (intelligence) and ACTION operation, or J-3 (Operations Directorate of the Joint Chiefs of Staff) functions.⁴ Some efforts to overcome these barriers with improved interagency communication techniques are discussed below.

The Interactions between Opposing Decision-Makers

The cycles of the warning process in Figure 1 are obviously generated by the actions emanating from opposing decision-makers. What we do affects what the opponent does, and what he does affects what we do.⁵ This phenomenon of interaction has profound implications upon the concept known as *intentions*.

Whenever a nation is contemplating a major political-military action, it must go through the series of decision steps suggested in Figure 2. First, the national decision-maker must be aware of his own capabilities (and limitations), of what he can (and cannot) do. Once he feels threatened by

3. For further discussion of these points, see, as a small sample, Jervis (1970), Snyder (1972), Milburn (1972), McClelland (1964), and the many excellent discussions of the Cuban missile crisis, e.g., Allison (1971).

4. For more on these barriers, see Boulding (1970: 85), Hilsman (1956), Barnds (1969), Ransom (1974), and Kent (1965).

5. Since this is not the place for a theoretical or methodological discussion of levels of analysis and their linkages, this rather cavalier connection will be allowed to stand. Crisis and warning can be examined from both perspectives, as illustrated by McClelland (1969, 1972a, 1972b) and Hermann (1969).

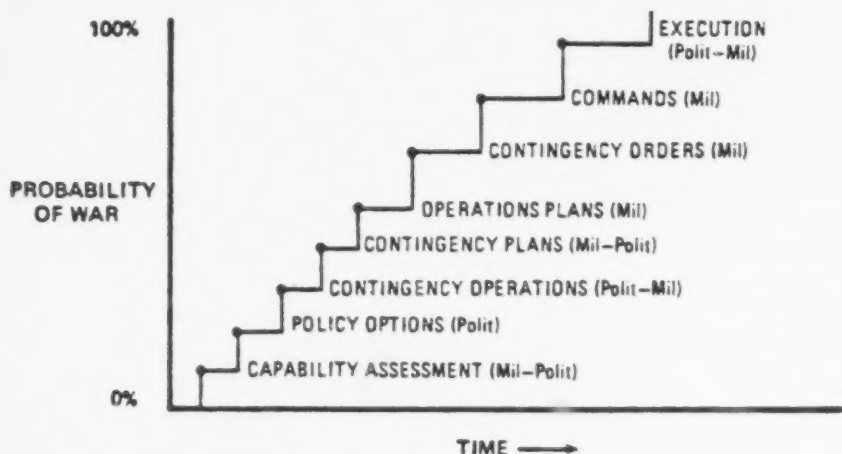


Figure 2: Decision Stairway

another nation, he must determine his policy options (what he might do if . . .). He must then examine contingency options and plans and, if the threat continues, move up the decision stairway with operational plans, orders, commands, and finally the command of execution. As illustrated by the recent attempt of the South Vietnamese government to disengage its troops in the north by precipitous action without proper planning, any decision-maker who avoids or skips these steps does so at his peril.

As one ascends this stairway, the probability of war increases. At any time, however, decision-maker B might take an action which alters the situation in such a way to cause decision-maker A to change his mind, "back off," and go down the stairway away from hostilities.

Consider the case of the events leading to the attack on Pearl Harbor as expressed in terms of the decision stairway in Figure 3. After a build-up of capabilities in the late 1930s, the Japanese attained the capability to dominate the Western Pacific. However, they also were engaged in a war with China, which generated hostile reactions from the United States (in the form of economic sanctions). The Japanese responded with contingency options and plans which, after our imposition of an oil embargo on Japan, led to the operational plans to attack Pearl Harbor. But negotiations with the United States were continuing even as Admiral Nagumo, the Japanese task force commander, was moving his fleet across the North Pacific toward Hawaii. He was sailing under contingency orders

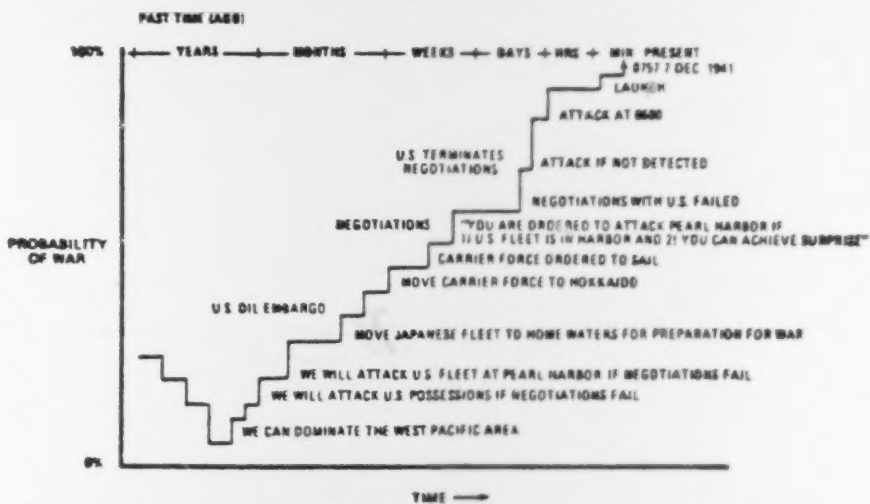


Figure 3: Japanese Decision Process Leading to Pearl Harbor

to attack the U.S. Fleet at Pearl Harbor if two conditions were satisfied: (1) the U.S. Fleet was in Pearl Harbor, and (2) he could achieve surprise. Nagumo was under the additional orders that if he were detected by the U.S. Navy down to 24 hours prior to the attack, he was to say that his task force was only on an exercise, and he was to bring it back to Japan.

If the U.S. intelligence system had been able to detect the approach of Nagumo's task force, and if our policy-makers had decided to let the Japanese know we knew they were approaching Pearl Harbor, then Nagumo would have been deterred from attacking. Given these circumstances, what could one have said about the *intention* of the Japanese to attack Pearl Harbor? The concept of intentions is not simple.⁶ Certainly the Japanese delayed the intention to attack as late as was feasible, using the standard decision technique of keeping one's options open as long as possible.⁷

The important point is that *the best any intelligence system can do is to determine where the opponent is on the decision stairway*. In many

6. The old debate over whether an opponent should be evaluated in terms of his capabilities or intentions continues. For views on the problem, see Brodie (1959: 378-379), Armbruster (1969: 223), Donnelly (1963: 6-9), Shlaim (1976: 362-365), and McClelland (1972b: 33-34).

7. Wohlstetter (1962), of course, provides an excellent analysis on the Pearl Harbor attack. See also Shlaim (1976: 378).

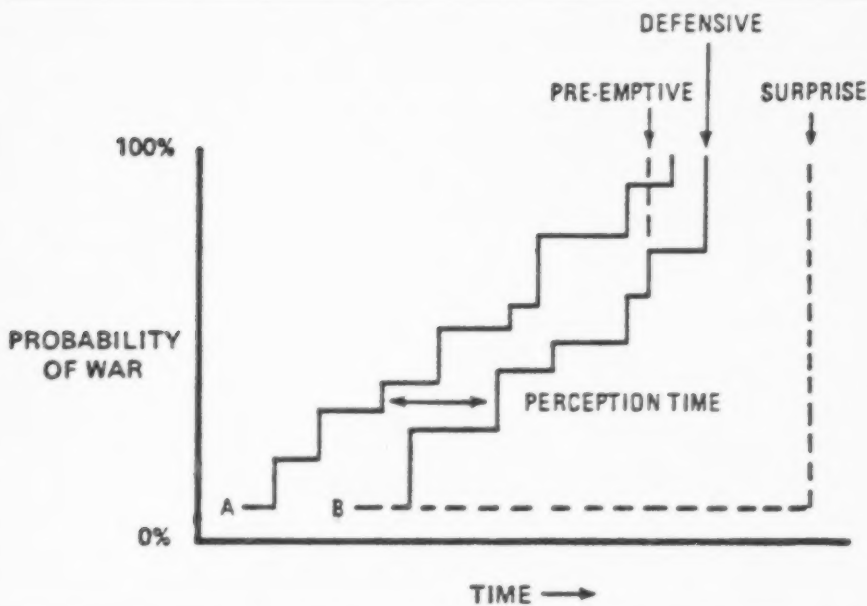


Figure 4: B's Response to A

circumstances, this determination can be used to take actions which will force the opponent to avoid conflict.

It should be remembered that one cannot make predictions of future events with absolute certainty, because the opposing decision-maker might not yet have made up his own mind whether or not to execute his plan. That decision might well depend on one's own actions.

Confusion also arises from the false dichotomy of whether the opponent is conducting an "exercise" or "a real operation." In the Pearl Harbor case, if the Japanese had been detected, the "real operation" would indeed have been an "exercise."

It is also possible for A to take an action which changes B's plans away from hostilities without A's ever knowing it. Conversely, it is possible for A's actions to be misunderstood by B, with subsequent hostilities resulting from miscalculation.

Interactions of Opponent Decisions

Figure 4 depicts the decision stairway of nation A and the decision responses of opponent B. The case in which B is not tracking A's decisions,

with the result being total surprise, is represented by the dashed line going out horizontally and then straight up.⁸ The other dashed line indicates a situation in which B not only tracks A's decisions but decides to preempt (e.g., Israel-1967). However, the usual minimum objective is the case where B tracks A's decisions well enough to be in a strong defensive position when A finally attacks.

There is, of course, a lag between A's decision at any given time, and B's own decision to respond. This lag, noted as "perception time," includes the time consumed for detection, analysis, and making the decision.

Figure 5 indicates a case in which B's responses to A's decisions eventually deter A's moves toward hostilities and cause A to "back off" and go down the decision stairway away from hostilities. The Cuban missile crisis is the classic example of this type of interaction. In that case, the decision stairway tracking was done well enough so that U.S. actions (and associated signals) deterred the Soviets. Although the missile crisis was a success from the U.S. point of view, it should be remembered that resorting to this kind of response can be very dangerous because of the potential for miscalculation by either side.

Figure 6 represents a situation in which A and B generate a confrontation between C and D. An example of these "second-order

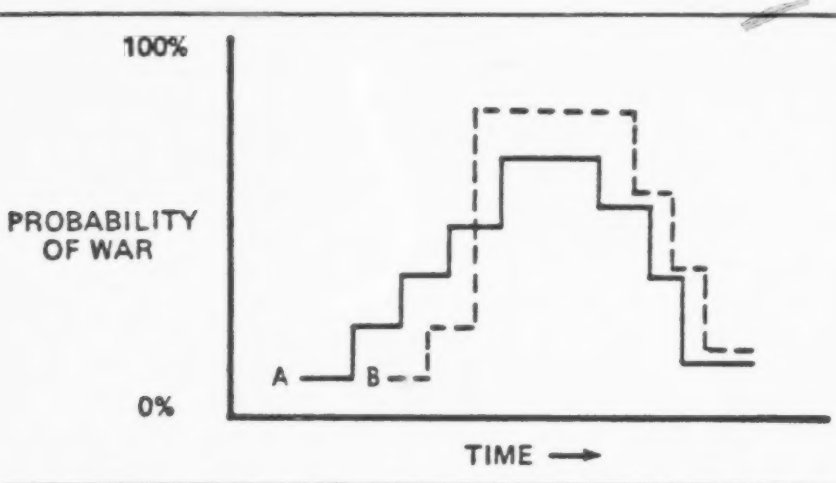


Figure 5: B's Response Deters A

8. For more on surprise, see Ben-Zvi (1976) and Shlaim (1976: 348-351).

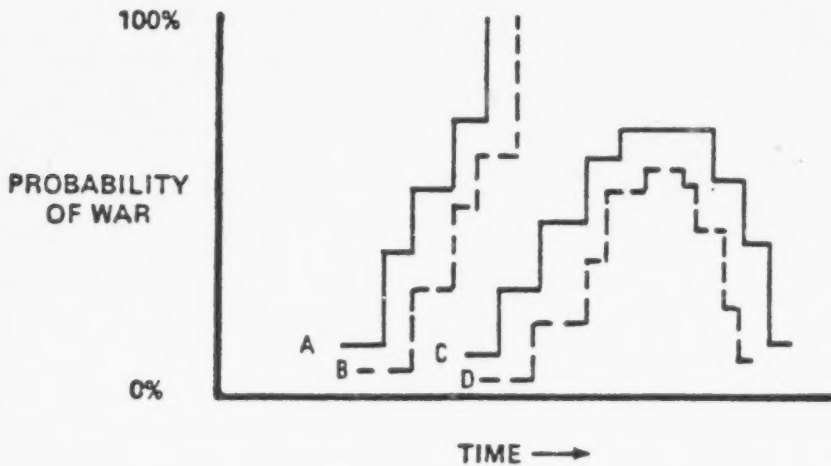


Figure 6: A versus B Triggers C versus D

crises" is the Yom Kippur War in the fall of 1973. In terms of Figure 6, A would represent the Arab nations, B the Israelis, C the United States, and D the Soviet Union. While C (the United States) had an intelligence interest in the developing hostilities between the Arabs (A) and the Israelis (B), there were no drastic decisions to be made by the United States until the period of the confrontation between ourselves and the Soviet Union.⁹ The big power confrontation arose after the war had started, specifically after 16 October, when the Israelis crossed the Suez Canal and eventually cut off the Egyptian Third Army (after apparently breaking two cease-fire agreements). The indicators of potential superpower involvement were generated primarily by the tactical ground situation on the west bank of the Canal between 16 and 26 October. In short, the warning of a confrontation between the major powers derived from a tactical situation arising from a localized conflict.

Organization for Detection of the Decision Stairway

Unfortunately the indicators generated in crisis situations do not come neatly packaged in political, military, economic, strategic, tactical, major power, and minor power categories. They are a mixture of all these

9. For the interactions of U.S. and Israeli intelligence, see Shlaim (1976: 360-361).

elements. It is even difficult to draw a line between the indications and warning phase, and the crisis or hostilities phase.¹⁰ The difficulty of trying to fit the 1973 Middle East crisis, illustrated by Figure 6, into these organizational concepts is shown in Figure 7. The horizontal line roughly indicates the division of the world into "strategic-tactical," a division that can cause problems when the "strategic" decisions at higher levels are generated by tactical events. The division between "I&W" (Indications and Warning) and "crisis ops" (crisis operations)—roughly, the vertical line on Figure 7—fails to cover situations in which one crisis generates another.

As illustrated in the major power confrontation resulting from the Yom Kippur War, the concept of "big W" versus "little w" (the distinction between major powers, e.g., USSR, CPR, and the United States as mutual opponents, and minor powers as opponents) also has obvious shortcomings. When would the "big W" mechanism have been turned on in that

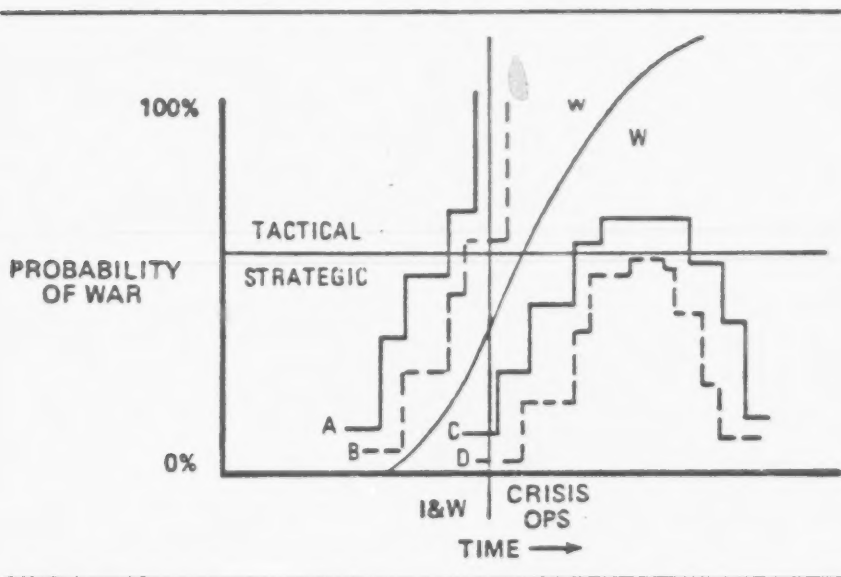


Figure 7: A versus B Triggers C versus D

10. Scholars of international politics have long studied crises and their phases from various perspectives. For diverse examinations and explanations of crisis phases and factors operating within the across these phases, see Lasswell (1965: 62-71), McClelland (1972b: 35; 1972a), Young (1968: 18-19), Wright (1965), Bloomfield and Beattie (1971), Bloomfield and Leiss (1969: 3-39), and Hermann (1969).

[192] INTERNATIONAL STUDIES QUARTERLY

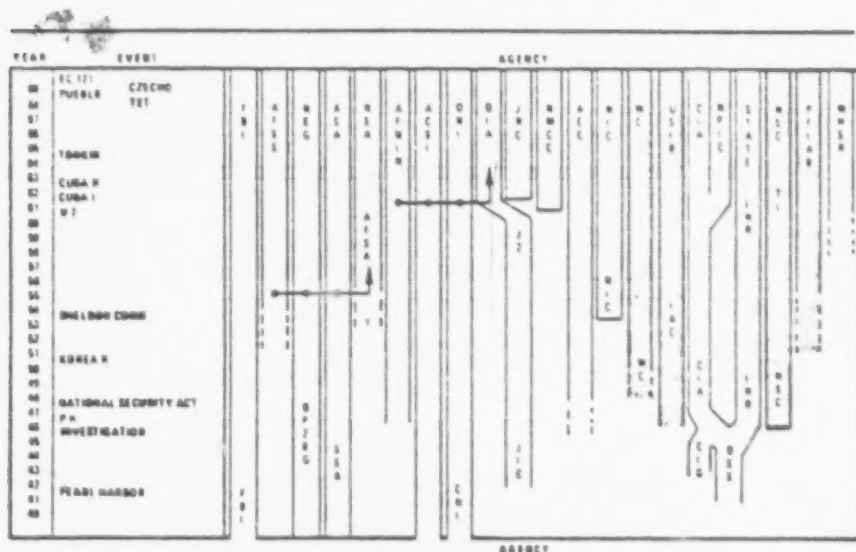


Figure 8b: Intelligence Organizations, 1940-1969

One conferencing system, which has recently become operational, is the National Operations and Intelligence Watch Officers Net (NOIWON) which allows the operation centers of CIA, DIA, NSA, State, State INR, J-3, and the White House Situation Room to call a secure voice conference at any time. Such a conference has three possible results. In most cases, the participants simply share information on a given situation which has come to their attention. However, if any one of the NOIWON members feels it necessary to take a particular action (such as notifying his agency director in the middle of the night or recommending that his organization go on some type of alert), he will notify the other members of the NOIWON. Finally, if any two watch officers decide that the incident is sufficiently important, they may issue an "Advisory" (a short formatted message describing what is known, and what is not known, about the incident). The Advisory is distributed upward, laterally, and downward through each organization. It not only gives information but also seeks feedback information on aspects which are unknown or ambiguous. Other NOIWON members may register dissent, but they are required to transmit the Advisory within their own organization.

A second type of conference can occur among analysts of the same organizations represented in the NOIWON (except the White House) and is known as the NOIAN (National Operations and Intelligence Analysts Net).

The NOIAN, a system now being tested, is chaired by the appropriate National Intelligence Officer (NIO) and uses secure voice in a conferencing mode. This system, called "Meet-Me-Bridge," is established by notifying each conferee to dial a predetermined number at an appointed time to begin the conference. No operator is required.

Another system now being developed which can be used by the NOIAN is CONTEXT (CONferenced TEXT editing), which allows secure voice (speaker phones) to be used in conjunction with a cathode ray tube (CRT) and a hard-copy printer. These devices, placed in a conferencing room at each major facility (CIA, Pentagon, NSA, and the State Department), will allow analysts who are specialists for a given tension or crisis area to create jointly a national situation report, a proposed alerting memorandum, or other documents of severe time sensitivity, without having to leave their own headquarters. The secure voice conference element of CONTEXT uses high-quality speaker phones in each CONTEXT room. The voice lines are connected, so that use of any CONTEXT phone automatically rings the others. The voice portion of CONTEXT can be used independently of the computer-visual data features. When used by itself, the voice element of CONTEXT becomes the equivalent of a "Meet-Me-Bridge."

Although improved communication techniques are not a panacea, they might help solve some of the organizational difficulties surrounding the inseparable functions of indications, warning, and crisis operations. However, the basic problem remains: given all the improvements in physical communication, what do people have to say to each other? How precisely do they say what they mean? One of the most difficult forms of precise expression is making warning statements in probabilistic terms.

Warning and Probability

The decision stairway (see Figures 3 through 7) is expressed in terms of time (horizontal axis) and probability (vertical axis). This requires that warning must also be expressed in these terms. The minimum expression of an interactive warning estimate must be in the form:

There is a _____% probability that A will act upon B by _____ (when).

There are many possible variations on this statement. First, probability can be expressed in terms of words, including auxiliary verbs and adverbs (might, might possibly, probably, and the like). Unfortunately, such expressions convey different meanings to different people. The uses of numbers (20%, probability, 3-to-1 odds, 4 chances in 10, and the like) are

[194] INTERNATIONAL STUDIES QUARTERLY

not without difficulties as well, particularly when used with false precision (e.g., 23.2%), but they do have the merit of internal consistency. Further, the choice of the number itself is not as important as the *change* over time of the number on a given estimate.

Below are listed some general principles governing probability statements:

- (1) *The more precise the prediction, the lower the probability.* If one says, "A will attack B on 16 September," that statement will have a lower probability than, "A will attack B in September."
- (2) *The greater the number of information elements within the probability statement, the lower the probability.* For example, "Three of A's divisions at X will attack two of B's divisions at Y on 16 September" will have a lower probability of being correct than "A will attack B on 16 September."
- (3) *The overall probability of the statement cannot be greater than the probability of any one element.* Using the first example in (2) above, if there is only a 30% probability that B has two divisions at Y, then the overall probability cannot exceed 30%.
- (4) *In general, the greater the time span of prediction, the lower the probability of its occurrence.* This requires that all probability statements include the date the prediction was made.

In making a probability statement, one must always keep in mind what one's own actions might do to the prediction. This holds even if one is not one of the two opposing parties. Some remarks should accompany the probability statement giving the assumptions regarding these potential interactions.

A warning estimate should always carry the name of the estimator and have provision for additional narrative information, sources, and other comments, including dissenting views.

Figure 9 is an example of a format for a warning estimate. Not all of the interrogatives of the information element (1 through 12) need be filled in. However, a minimum of subject (3), verb phrase (6), object (9), and time (11) are essential in an interactive warning estimate.

At any given time, an analyst might write several warning estimates related to the situation. This will allow him to review the estimates periodically and record any changes in the probability and the reason(s) for the change. The changes can be used to "take the temperature" of the situation. To do this, one must use precisely the same form of probability statement in the reassessment over time.

INDICATIONS, WARNINGS
AND
CRISIS OPERATIONS

Warning Estimate

Information as of:
Time of Release:
Identification No.

FROM:

TO:

THERE IS A 30% PROBABILITY THAT:

1. HOW MANY: Three
2. (OF) WHOSE: of A's
3. WHAT/WHO: divisions
4. WHERE: at Y
5. WHEN: - - -
6. (VERB PHRASE): will attack
7. HOW MANY: two
8. (OF) WHOSE: of B's
9. WHAT/WHOM: divisions
10. WHERE: at Y
11. WHEN: on 16 September
12. HOW + CONJUNCTION:
13. SOURCE(S):
14. ADDITIONAL INFORMATION:
15. COORDINATION COMMENTS:

Phone No.:

16. PREPARED BY:
(Security Classification)

(Security Classification)

Figure 9: Indications, Warnings and Crisis Operations

The importance for the policy-maker-consumer of accepting probabilistic warning estimates cannot be overemphasized because they relate to the type of decision (from drastic down to none) he is attempting to make. He

should also remember that if the kind of decision at hand does not require an estimate of great precision, a higher probability might be expressed. One possibility is for the consumer and the intelligence analyst responsible for a warning estimate to confer and agree on a series of basic probability statements and, without changing the wording, to review from time to time the changes in the probability and the reasons why the changes occurred.

Summary

Warning and crisis operations should be the most vital functions of the intelligence, diplomatic, and military organizations of our government. As evidenced by our performance in past crises, our national nervous system is not designed for a coherent response in most situations. We do not fully understand the warning process nor do we have complete knowledge of how our nervous system functions. Not only do we fail at human communications within our system, but we fail to perceive the interactions between our decision-makers and our opponents. We fail to express our estimates in probabilistic terms and relate these estimates to the kinds of alternative decisions that can be taken.

None of these shortcomings can be overcome by simple panaceas. However, there are remedial steps which can be taken, particularly in the area of more precise communication across the diverse parts of our government. These remedies cannot be effectively administered by any one segment (diplomatic, intelligence, or military), but they must be done in concert if we are to forecast-warn, avert, and effectively manage crises.

REFERENCES

- ALLISON, G. T. (1971) *The Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown.
- ARMBRUSTER, F. C. (1969) "The problem of China," pp. 221-234 in J. J. Holst and W. Scheider, Jr. (eds.) *Why ABM? Policy Issues in the Missile Defense Controversy*. New York: Pergamon.
- BARNDS, W. J. (1969) "Intelligence and foreign policy: dilemmas for a democracy." *Foreign Affairs* 47 (January): 281-295.

- BEN-ZVI, A. (1976) "Hindsight and foresight: a conceptual framework for the analysis of surprise attacks." *World Politics* 28 (April): 381-395.
- BLOOMFIELD, L. P. and R. BEATTIE (1971) "Computers and policy-making: the CASCON experiment." *J. of Conflict Resolution* 16 (March): 34-45.
- BLOOMFIELD, L. P. and A. C. LEISS (1969) *Controlling Small Wars: A Strategy for the 1970's*. New York: Alfred A. Knopf.
- BOULDING, K. (1970) "Social systems analysis and the study of international conflict," in A. Buchan (ed.) *Problems of Modern Strategy*. London: Chatto & Windus.
- BROADIE, B. (1959) *Strategy in the Missile Age*. Princeton, N.J.: Princeton Univ. Press.
- DONNELLY, C. E. (1963) *U.S. Defense Policies in 1962*. Washington, D.C.: Government Printing Office (for the Legislative Reference Service, Library of Congress).
- HAAS, M. (1974) *International Conflict*. Indianapolis: Bobbs-Merrill.
- HERMANN, C. F. (1975) "Indicators of international political crises: some initial steps toward prediction," pp. 533-543 in E. E. Azar and J. D. Ben-Dak (eds.) *Theory and Practice of Events Research*. New York: Gordon & Breach.
- (1969) "International crises as a situational variable," pp. 409-421 in J. N. Rosenau (ed.) *International Politics and Foreign Policy*. New York: Free Press.
- HILSMAN, R. (1956) *Strategic Intelligence and National Decisions*. Glencoe, Ill.: Free Press.
- HOLSTI, O. R., R. A. BRODY, and R. C. NORTH (1969) "Measuring affect and action in international reaction models: empirical materials from the 1962 Cuban crisis," pp. 679-696 in J. N. Rosenau (ed.) *International Politics and Foreign Policy*. New York: Free Press.
- JERVIS, R. (1970) *The Logic of Images in International Relations*. Princeton, N.J.: Princeton Univ. Press.
- KENT, S. (1965) *Strategic Intelligence for American World Policy*. Connecticut: Archon.
- LASSWELL, H. D. (1965) *World Politics and Personal Insecurity*. New York: Free Press.
- McCLELLAND, C. A. (1972a) "The beginning, duration, and abatement of international crises: comparisons in two conflict areas," pp. 83-108 in C. F. Hermann (ed.) *International Crises*. New York: Free Press.
- (1972b) "Some effects on theory from the international event analysis movement," pp. 15-44 in E. E. Azar, R. A. Brody, and C. A. McClelland (eds.) *International Events Interaction Analysis: Some Research Considerations*. Beverly Hills, Calif.: Sage Professional Papers in International Studies 02-001.
- (1969) "The acute international crisis," pp. 93-117 in K. Knorr and S. Verba (eds.) *The International System: Theoretical Essays*. Princeton, N.J.: Princeton Univ. Press.
- (1964) "Action structures and communications in two international crises: Quemoy and Berlin." *Background* 7: 201-215.
- MILBURN, T. (1972) "The management of crisis," pp. 259-280 in C. F. Hermann (ed.) *International Crises: Insights from Behavioral Research*. New York: Free Press.

[198] INTERNATIONAL STUDIES QUARTERLY

- RANSOM, H. H. (1974) "Strategic intelligence and foreign policy." *World Politics* 27 (October): 131-146.
- SAFRAN, N. (1974) "The war and the future of the Arab-Israeli conflict." *Foreign Affairs* 52 (January): 215-236.
- SHLAIM, A. (1976) "Failures in national intelligence estimates: the case of the Yom Kippur War." *World Politics* 28 (April): 348-380.
- SNYDER, G. H. (1972) "Crisis bargaining," pp. 217-256 in C. F. Hermann (ed.) *International Crises: Insights from Behavioral Research*. New York: Free Press.
- WOHLSTETTER, R. (1962) *Pearl Harbor: Warning and Decision*. Stanford, Calif.: Stanford Univ. Press.
- WRIGHT, Q. (1965) "Escalation of international conflict." *J. of Conflict Resolution* 9 (December): 434-449.
- YOUNG, O. (1968) *The Politics of Force*. Princeton, N.J.: Princeton Univ. Press.

Mr. GORE. Thank you very much.

What you are saying, in essence, is, our ability to deal with critical and useful information during a crisis often depends upon a preplanned network of communication which brings together the key analysts or people in each of several subloops and affords the opportunity for those key members of the subloop to interchange with each other and in so doing identify the most critical bits of information that will be useful to the decisionmakers in the heat of the crisis.

Mr. BELDEN. Yes. I don't know that it is preplanned so much. It is taking advantage of the system that exists and having knowledge of what all of these various communications systems are, and taking advantage of people who know people.

Two things: I use the term national nervous system to try to describe this problem. To find out what the national nervous system is, you don't look at organization charts or communications wiring diagrams. You look at the 24-hour watch centers. Who are they? Where are they? Who do they talk to? Who do they fail to talk to? There are many of them. In 1973, I made a list of 29 24-hour watch centers just in the Washington area. I made it up and sent them each a copy. They were shocked and amazed that each other existed.

We then got them together informally to have a drink together to know each other as people. This informal group is still going on every 6 months. At least they get to know each other a little bit.

Actually, there are hundreds of 24-hour watch centers. We made an effort to make a directory of these 24-hour watch centers. General Scowcroft was then in the White House, and we asked him to make a data call on all of the agencies, and nothing happened until *Mayaguez*. The *Mayaguez* trauma gave us the opportunity.

You know, *Mayaguez* was the perfect example of a missed opportunity of crisis avoidance. Eight days before the *Mayaguez* incident, the South Koreans had had trouble in the same area. They knew their own national nervous system well enough to be able to give warning to their merchant fleet. We intercepted that traffic. We knew they had done this, but nobody in our Government seemed to know who it was that could give warning to the merchant fleet of our own country. Obviously it is the Hydrographic Office's Defense

Mapping Agency that gives warning to the merchant marine. But you don't know this unless you have a directory and unless you know the system. This was how we were able to get General Scowcroft to make the data call. FEMA then published for us a list, one page for each watch center, 133 24-hour watch centers, the major ones. This has not been kept up because there is no intelligence community staff any more to keep it up.

It is tools like this that can take advantage of the system that exists because every crisis is different, and you have to use different parts of the national service system to bring it together.

Mr. GORE. In that instance it was in a sense preplanned. You identified the key person in advance of the emergency which triggered the need to pulse each one of them.

Mr. BELDEN. You mean in the *Mayaguez* case?

Mr. GORE. Yes.

Mr. BELDEN. We never gave warning to the merchant fleet. That is why we had the crisis. Nobody knew that much about the system.

Mr. GORE. If you look at the Three Mile Island incident as an example from a different arena, it would have been helpful, in the context of yesterday's hearing, if FEMA had had computerized data from National Weather Service, the Census Bureau, the other data bases that were mentioned, GEODEST files, and so forth. But it might have been even more helpful if FEMA had a preplanned network of key people in those agencies and was able, when the incident occurred, to pull out a card identifying those people, where they were, get them on a hookup, get the data to them to analyze and share with each other during the emergency, and then feed that to the NRC and the Pennsylvania State authorities on a timely basis.

Mr. BELDEN. I agree with you totally. That is a people-retrieval problem, and I think that is one of the things we don't do enough of. We tend to try to retrieve data. The big thing is to retrieve people. The second big thing is, if you are in a great hurry, how do you connect them together?

Mr. GORE. I really find your testimony extremely valuable, because yesterday I was grappling with this enormous logistical problem of getting all these disparate data bases in a form that made them accessible quickly to the decisionmakers. Of course, as you point out, the key to any such system is people, and the way to short circuit that process is to loop together the key people who have a preexisting understanding of the data bases involved and are able to quickly sort through the mass of data available in that subloop, where they are found, and extract from it the most important bits in a form—voice communication—that is most easily useful by the others in the network and the decisionmakers who will be looking to that network.

I think your model is of crucial importance.

Mr. BELDEN. I agree with you. Also, when you try to make disparate data bases compatible, indeed theoretically this can be done, but, as Mr. Hicken will tell you, everybody is changing his data base all the time, and you can't get all the answers to line up right. But you can do one thing, and that is to retrieve people.

Mr. GORE. Mr. Walker?

Mr. WALKER. Did I understand from your testimony this is a problem in all of this business of putting together a group of people, however, in that even if you get a communications system that allows you to do that, that you are going to have problems with that group of people in that the analysts or the professionals, or whoever you bring in, are very uncomfortable about making a judgment that all of their professional colleagues throughout the whole community will either accept or reject almost immediately—that we do have that very, it is almost an institutionalized people problem?

Mr. BELDEN. Yes. It is not only their colleagues; it is their superiors that are going to be considered cut out of the loop. The only time this successfully happens is when the crisis is severe enough and there is enough pressure from the Executive Office of the President: In other words, in the Cuban missile crisis, for example, if you will recall, the President did not take the DCI's word for it about the missiles. He demanded to see the photo-interpreter in his office, to bring the pictures, to explain. Now, this ruffled all kinds of bureaucratic feathers, but it happened because it was the pressure. The point you are making is absolutely correct. It is not only colleagues but also superiors.

Mr. WALKER. Is there also a fear, too, that if they make a misjudgment, or if they analyze the data incorrectly, that in terms of all of their colleagues, their superiors and everybody else, that they will be held up to ridicule? Going back to Three Mile Island, how about the guy who made the judgment about the hydrogen bubble that existed in the reactor and had the whole Government running around talking about this great crisis that never existed. Is there a problem in that kind of situation?

Mr. BELDEN. Yes, sir, there is. However, in the intelligence world at least, I think the analyst has to have the right to be wrong. Otherwise, he will never say anything. It is a very tricky game. You can't expect him to have a 1.000 batting average. If he bats .300, he is doing very well. If you demand that he bat 1.000, he is not going to go to bat. It is that simple. You have to have the right to be wrong in this business.

Mr. WALKER. I understand that except it seems to me if you are faced with a crisis of fairly short-term dimensions, that then the analysis is going to be followed almost precisely because there will be very little opportunity to backstop that and find out that on this—he may be batting a good average of .300. The only problem is in the short term it was one of the times he struck out and we are on a collision course, then, with some very grave realities.

If you are faced with something where—well, again, Three Mile Island, where many people were led to believe that they were in immediate danger of having their homes and their farms and everything else wiped out by an explosive atmosphere within the containment.

Mr. BELDEN. That is true. However, had it been a dangerous situation, you would have been glad he did it. In other words, he erred on the side of conservatism. It was an error. There is no doubt about it.

Mr. WALKER. Except in that particular instance it turns out that when we got the real experts in, when you got the actual cast of

characters, the people who put it through, there was no way that situation could have ever existed in there because there was no way for hydrogen to build up in the way it was previously described, so, in fact, a totally unreal characterization was put out as being the basis of the crisis.

Mr. BELDEN. I am not familiar with Three Mile Island, but it appears to me to be a case where if you had been able to retrieve the right people and conference them at the time, you might have been able to avoid that.

Mr. GORE. If my colleague will yield.

Mr. WALKER. Glad to.

Mr. GORE. In the context of the specific example, if experts at the nuclear reactor companies and in the departments of some of the leading universities had been given the data quickly and tied together in a conference arrangement, the initial mistake might have been quickly identified.

Mr. BELDEN. I think that is right.

Mr. WALKER. And it became very clear that once they began to use the experimental reactor in Idaho and ran through a scenario of what had taken place at Three Mile Island, then we began to get very good data. Had that been made earlier, it might have been a case where we would have had better information with which to work.

With each crisis you have a different kind of situation, so you will have a differing cast of characters we have to bring in in each instance.

How do we put together the contingency plans that allow us to assure ourselves that the cast of characters we assemble in each crisis is, in fact, a proper one, and we don't leave out somebody who might be of vital importance in a crisis that, of course, we can't identify in our contingency plan?

Mr. BELDEN. You bring up a very fundamental problem, and that is the whole area of contingency planning.

Now, I think it is a good process to do, provided you never believe in the plan. You never believe that things are going to happen that way. I have seen cases in the intelligence world where the data is selected on the basis that it fits the contingency plan. There is what I call seductive reasoning, as against inductive or deductive. In other words, it is reasoning that allows one to collect the data that fit the desired conclusion.

A contingency plan can do that. Now, contingency planning is a good process to let you know how to plan. If you can free your mind from it when an event occurs and say, "I have never seen anything happen according to the contingency plan, but I know how close this is to such-and-such a kind of thinking we did before, and I can take advantage of that."

To try to make a contingency plan for every contingency is futile. Man's ability to read the future is not that good.

Mr. WALKER. But isn't a flawed plan better than no plan at all?

Mr. BELDEN. Oh, yes; but having made the plan is what is good. Having gone through the process of making the plan. Because then you know how to plan and replan quickly.

Mr. WALKER. It still seems that it comes down to the point that somewhere along the line, though, you have a crisis and you are

going to pick the cast of characters, you are going to pick the people you are going to depend upon to get you through the crisis. In the course of that, you are going to pick one key player. Somebody is going to end up being the focal point, the decisionmaker in all of this, and I guess it comes down to the question of how do you assure that you have that right person.

Again, I will come back—since I have lived with Three Mile Island and still live with it all the time, it turned out the most important player in Three Mile Island was not the fact that we picked somebody who had precise expertise of precisely what was going on there, but we picked a pretty good public relations man—I mean, a guy who got up there and got a little bit of public confidence on his side and on the side of the people who were trying to handle the crisis.

I don't know that that would be the case in each and every instance. In some cases you would want to pick the person with the greatest technical expertise. How do you assure yourself that you have some degree of preciseness or at least some degree of good judgment in picking that key player?

Mr. BELDEN. Well, again, I think, picking that key person is absolutely dependent upon the peculiarities of the crisis that you are in. It is very unpredictable as to who that would be.

You have to have somebody who has the confidence of the next higher level. I think that is essential. It doesn't surprise me that they would pick a public relations man in the type of crisis you describe, because the public was deeply involved, so it seems rather natural to me.

In another case it might be somebody with expertise, but again it depends upon the particular crisis.

Mr. WALKER. The Joint Chiefs regularly draft, and then they update contingency plans for military operations. How much of that do we actually do in the civilian community?

Mr. BELDEN. Well, I have seen some. I think they are much more sketchy. I think the Joint Chiefs have the advantage of a very well-defined national command authority and chain of command on the action side. As I said before, the difficulty is on the upside. Whether other nonmilitary agencies have that clear cut a command chain and doctrine to go with it, I don't know.

Mr. WALKER. What would you have to say on the question of the Soviets now building a massive civil defense capability? We have almost gone out and dismantled ours. It is almost nonexistent in some communities.

Are there any particular consequences in either the activity in which they are engaged in terms of their decisionmaking capabilities, or the consequences of our actions in dismantling what we had in place?

Mr. BELDEN. These are just my own private views on this matter. This is one of the asymmetries between ourselves and the Soviet Union. I think civil defense pays a large dividend to an aggressive nation because he can give himself warning. It is that simple. He knows when he is going to attack and therefore he can use his civil defense system.

The defender has a great disadvantage here because the opponent can spoof the system too easily. It is so easy, you know, to

holler "wolf" by disinformation and exercise our civil defense system until it just won't respond any more. So the question you raise, of course, is much more complex than that simple answer I have just given.

Mr. WALKER. Do I interpret correctly that civil defense is the better part of a good offense than it is defense?

Mr. BELDEN. In my opinion—the best part of defense to me is to have your missile systems, for instance, able to produce a number of aim points that are so large to the opponent that he cannot digest them in the time of his own intelligence cycle. I might add, as a private citizen, my disappointment in the apparent decision about accepting the MX race track deployment system that has been made today. But that is another whole subject, and I would rather not go into that at this time, but I have very powerful feelings about it. However, it is related to your question of civil defense.

Mr. WALKER. Because of the number of aim points and issue points?

Mr. BELDEN. Yes.

Mr. WALKER. One final question. It seems far too often in a critical situation where there is a lot of important occurrences, that we have information available but for one reason or another it gets ignored. We have the base of information, we may even have the people in place, but the right people get ignored or the information, itself, gets ignored. How do you think we overcome that?

Mr. BELDEN. As I mentioned earlier, in the postmortems I have done—unfortunately, there isn't time to go into those—but every time, that phenomena occurs. There is always this massive amount of critical, relevant information in the system that never gets used, and it is partly, I think, a people-retrieval problem.

Mr. WALKER. You are saying if you have the right people in place, the chances are they will get the right information, whereas if you have the wrong people, it will almost be by chance that they get the right information?

Mr. BELDEN. Yes. I will at least say if you get people retrieval, the probability of getting the right information will go up. It doesn't guarantee it.

Mr. WALKER. Thank you, Mr. Chairman.

Mr. GORE. Mr. Shamansky?

Mr. SHAMANSKY. Thank you, Mr. Chairman.

Dr. Belden, sort of on a more modest scale rather than the strategy with respect to MX, which is something rightly we are not able to do much about, at this level, what are your views on the willingness or the reluctance of key personnel involved in planning for predictable emergencies in the sense that there are going to be so many in the Midwest and so many in the Southwest, like tornadoes and floods, to share vital information. What is your experience and views on something like that?

Mr. BELDEN. Unfortunately, my experience has been primarily in the military world.

Mr. SHAMANSKY. How does it work in the military world?

Mr. BELDEN. There is a great deal of reluctance to share information.

Mr. SHAMANSKY. Why?

Mr. BELDEN. Let me bring up an example of the problem of the transfer of information between the intelligence or J-2 side of the House with the operations, or J-3 side of the House. I alluded to this somewhat earlier. In many times we have had to conduct intelligence on our own forces to know what we are doing in order to be able to respond at the right time at the right place, because of the reluctance of interchange of information.

Mr. SHAMANSKY. I am asking you to identify the source of the reluctance. You state there is reluctance, but I want to know why you think there is reluctance.

Mr. BELDEN. I discussed this with the J-3 General Le Van in 1977, when he had that office, and I have been trying for a long time to make a treaty between the intelligence community and the J-3.

Mr. SHAMANSKY. A treaty?

Mr. BELDEN. Well, in my terms.

Mr. SHAMANSKY. It is a word of art; it is all right.

Mr. BELDEN. General Le Van said, "I would be willing to give you—"; you see, ideally J-3, before he went into an operation, when he was considering his contingency options, ideally he would go to the intelligence world and say, "If we did A, B, or C, what would be the responses?" That would be nice.

The next nicer thing would be when he chose an option to tell the intelligence community which option he chose. That wasn't done. Finally, once he executed, to tell us that he has executed the option.

Now, General Le Van said, "I would be willing to give you the first step to let you consider the options and tell us what the reactions would be." He said, "What I don't want is for the intelligence people to be in the act earlier than that, when we are just brainstorming the problem, because if we are not free to think about the problem in our own way, the intelligence man is going to go back to the community and say, 'Do you know what those crazy people are thinking about doing?'"

So he was willing, once they selected options, to tell the intelligence community. I thought this was a good agreement, and I thought his reason for reluctance at that earlier stage was a reasonable one. But at that time, the intelligence community staff had more or less lost interest in the question, and I could not finally make the connection.

Mr. SHAMANSKY. When you worked on this treaty, did you call a peace conference?

Mr. BELDEN. Virtually.

Mr. SHAMANSKY. How do you bring that off?

Mr. BELDEN. It is very difficult.

Mr. SHAMANSKY. It is a mechanical sort of thing?

Mr. BELDEN. Yes.

Mr. SHAMANSKY. If you are having trouble in the military, where theoretically you have a chain of command and responsiveness, where I am major general-somebody and you are only brigadier general, you would think you would have some kind of pressure for responding to orders. You couldn't bring it off in the military.

Mr. BELDEN. No, sir. Of course, the intelligence community staff is not really a military organization; it is a civilian organization. It is the interface there that is difficult.

Mr. SHAMANSKY. I gather from that you are sort of gloomy about—if they were all civilian agencies—are they reluctant to share their information?

Mr. BELDEN. I have seen instances of that, but I must say that I am not as familiar with the civilian agencies—

Mr. SHAMANSKY. Carrying on this practical thing a little further, do you think it would make sense to have some sort of permanent disaster testing and evaluation center that itself would not be a permanent disaster? Is that possible?

Mr. BELDEN. If I may take the analogy into the military world, the intelligence-military world, the same principle of having a big center, so to speak—

Mr. SHAMANSKY. I am not pushing the idea. I just want to know what you think.

Mr. BELDEN. My reluctance about that is the same as it was in the military world. There was a suggestion to have a great big indication and warning center that took care of all foreign crises, and so forth. It sounds so good until you think about the fact that every crisis is different. And so you can't have a center of people who are experts about everything at all times.

Mr. SHAMANSKY. How would you then prepare? Would it make sense to undertake simulated tests just to get people thinking about some kind of a—

Mr. BELDEN. Oh, exercising, yes, is a very good thing to do.

Mr. SHAMANSKY. Who would coordinate the exercise, or does there need to be coordination?

Mr. BELDEN. There needs to be coordination, but our exercises right now—

Mr. SHAMANSKY. Coordination?

Mr. BELDEN. It is done on a voluntary basis. For instance, in the exercises that the JCS runs, they coordinate with, say, the FAA, to be part of the exercise. That is just an interagency coordination with no superior involved, and it has been successful. I think it is very important.

Mr. SHAMANSKY. Then the solution may be not to have a superior involved.

Mr. BELDEN. In some cases, yes. I think if you can find areas where there is mutual interest.

Mr. SHAMANSKY. How could there not be mutual interest in the disaster? How would this not be mutual interest?

Mr. BELDEN. I agree.

Mr. SHAMANSKY. Then how do you motivate these people to act rationally in that situation?

Mr. BELDEN. Well, to motivate them, unless it comes from higher authority—

Mr. SHAMANSKY. We are trying to establish how we get higher authority to be cognizant of these problems and get results. Even in the exercises.

Mr. BELDEN. Well, for years, higher authority has been criticized for not participating in any exercise. I think participation by the higher authority in a few exercises is a very good thing, and it

makes them conscious of the problems, and that is where the motivation would come from.

Mr. SHAMANSKY. Mr. Chairman, maybe we would have a role in inspiring higher authority to have these exercises.

Mr. GORE. We are going to publish a report with specific recommendations, and, as I mentioned at the outset of the hearings, Dr. Beal, at the White House, and Mr. Meese, are following it very closely, and we have every expectation of making a substantial contribution to change in a positive direction in this area.

Thank you very much for your appearance here today, Dr. Belden. We could go on with you for some time. You are a fascinating witness. However, we are behind schedule and will have to do some catching up.

Thank you very much for coming and enlightening us.

Dr. Robert E. Kahn is our next witness. He is Director of the Information Processing Techniques Office of the Defense Advanced Research Projects Agency at Arlington. Dr. Kahn, welcome. We are delighted to have you, and please proceed with your presentation.

STATEMENT OF ROBERT E. KAHN, DIRECTOR, INFORMATION PROCESSING TECHNIQUES OFFICE, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, ARLINGTON, VA.

Dr. KAHN. Mr. Chairman and members of the subcommittee, I am very pleased to be with you this morning. What I would like to do is to discuss with you a variety of aspects of information processing technology as it applies to the problem of emergency management.

I will try to address my comments to higher-level concerns rather than get into technology details which we could do at some later time if it were of interest to the subcommittee. I will try to highlight the various technologies, how they might be used, to briefly describe them and to place them in context so you can see how they might apply in various situations.

I am happy to be following Dr. Belden's testimony, because, in fact, I also believe that the human aspects of manning any crisis, whether it be civilian or military, is, in fact, the first order of importance, and that technology can facilitate, in fact it may be critical to, the carrying out of those functions by human beings. But without the human capability in the loop, nothing useful is going to happen. This is really a description of technologies which can augment people and their ability to cope with crises and deal with management in various emergency situations.

In general, I think there is a fundamental question to be asked about the role of technology in this whole process. You have probably heard not only in this session but many times before about the rapid progress that we have been making in technology, but yet I think it is still very unclear what role computer technology, for example, should play in emergency management. What role should be taken by technology in dealing with crises, what role should people play independent of the technology? In some very limited sense one might think voice communication was all that was really required; in times of crisis. If people can deal with the problem, the presumption is they need nothing more than the ability to talk with other people. And yet while that is the mainstay of many of

our most significant crisis management systems today, it is by no means the end of the line. In fact, it is more like the tip of an iceberg.

We all know about the limitations of the telephone. Sometimes you can't get the party at the other end; sometimes the data that you are interested in accessing can't really be presented properly over the telephone. Graphics might play a role, or whatever.

We are interested in how information-processing technology can be used, what role it can play. We are interested in how people can use it to react effectively to certain problem situations. We are especially concerned about the fact that access to certain kinds of information in an emergency situation may be critical. It may be the determining factor in our ability to deal with that crisis.

Knowing where food or medical supplies might be, knowing what the status of various facilities might be, and so forth. That probably means participation by a large number of people and probably on a regular basis in order to keep that kind of information up to date. It may be required during the crisis; it may be required before or after. In any event, it certainly involves the participation of a large number of people and large amounts of equipment as well, sensor equipment, for example.

Finally, we are concerned about issues of planning. Given that you have enough, or whatever information you can obtain, how do you put together a reasonable plan and keep that plan up to date? How do you replan when appropriate to deal with an evolving situation? How do you disseminate the information from that plan, either to cause actions to be taken or, more importantly, to deal with just general information-informing the public at large, for example. It may turn out that the single most important factor in keeping a crisis under control is adequate information to the public at large.

There was an emphasis in the first talk this morning on what I consider to be the strategic problem, in which you have enough opportunity to assess a problem while it is arising, where you can take various actions to hopefully allay it or place it in one context or another.

But there are also many emergency situations where the warning is almost negligible and where you have to react with either people or facilities that are essentially in place or that can be transported very, very quickly. In these situations, you may not be able to get experts to deal with the problem but simply must use the resources that you have at hand. I think this is characteristic of many civil emergencies in the past.

I am not going to dwell on some of the basic technologies which I think are essential in this area such as, the whole development of semiconductors. We all know this has been a major growth industry in the United States and around the world. It is absolutely critical to many of the technological capabilities that we will see emerging in the future and to those which exist today in the computer field and the communications field. But that is a matter of a whole other discussion, and I am not going to be discussing that subject matter this morning.

[Slide entitled "Information Processing Technology for Emergency Management" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

ASSUMPTIONS

- DEALING WITH DOMESTIC CRISES
- NOT DEALING WITH INTERCONTINENTAL OR INTERNATIONAL ASPECTS (WHICH ARE PERHAPS UNIQUE TO DEFENSE)
- CRISES NORMALLY HANDLED BY STATE AND LOCAL AUTHORITIES WITH POSSIBLE FEDERAL LIAISON

Mr. KAHN. My talk this morning will be on information processing technology. The second slide indicates some of the assumptions I will make in the presentation. First, we really are talking about domestic crises of one sort or another. In particular, we are not dealing with international or intercontinental kinds of issues, and specifically not those that typically would be handled by defense. Defense may play a role in a domestic kind of problem, but we are not talking here about launching AWACS aircraft or carriers at sea or that kind of situation.

We are talking about crises which normally would involve the local authorities in one form or another. In these situations, there may need to be some appropriate information, reporting or even action-link back to Federal authorities, but for the most part, this is a localized kind of crisis in which we need to take some action on very quickly.

[Slide entitled "Information Processing Technology for Emergency Management" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

EXAMPLES

- **NATURAL DISASTERS**
- **TERRORIST ACTIONS/THREATS**
- **RIOTS AND NON-PEACEFUL DEMONSTRATIONS**
- **TECHNOLOGICAL EMERGENCIES**

Mr. KAHN. Some examples that come to mind are, (1) Natural disasters of various kinds such as hurricanes, tornadoes, earthquakes, or whatever, (2) Terrorist actions and threats I think are of a fairly specialized kind, and I would like to come back to that a little later in the context of some of the security requirements which I think apply to that case, (3) Riots and various kinds of demonstrations which are meant to be disrupting, I think, would fit into another category. (4) Finally, there are a whole variety of technological emergencies that I might have called industrial emergencies instead. They could range from the failure of an industry, power outages across the country, things of that form. Three Mile Island would probably fit more in that latter category than any of the others.

[Slide entitled "Information Processing Technology for Emergency Management" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

INFORMATION PROCESSING

- COMMUNICATIONS
- COMPUTERS
- ARTIFICIAL INTELLIGENCE
- SECURITY

Mr. KAHN. These are the four areas I am going to focus my discussion on this morning. They are not the only information-processing technology areas which are relevant, but they are four that I think are highly relevant, perhaps the four most important on the list. Let me briefly talk about each.

The first is the communications area. I don't need to remind you about the crucial importance of making it possible for people to talk to other people. It is also important if we have computer-based systems which have crucial information that we be able to communicate with them as well. The most significant recent development in the communications arena in my opinion has been the development of technologies which greatly facilitate our ability to communicate with computers as well as with other people and to make it possible for computers to communicate with other computers in the process of developing their data bases and getting that information back to humans.

In the case, for example, of a distributed data base system, a single query of that system could conceivably result in dozens if not hundreds of interchanges between different data-base systems to form the right answer, to get the most relevant information to the right place.

That all requires some kind of network technology, and I am going to spend some time talking about the implications of relying on networks for communication. I think they are absolutely essential in handling emergencies, and they can support both people-to-people, computer-to-computer, and people-computer interactions. The difference between interacting between people (say by voice) is

that small errors in transmission tend not to make too much difference since you can always ask a person to repeat something. You need the same kind of mechanism built into a computer communications medium to make conversation between computers effective. They cannot tolerate, even in some cases, single bit errors, particularly if you are moving programs and files around.

The nature of the communication medium wants to be somewhat different, in some cases significantly different, than that which you would experience in normal communication between people. It wants to be as error-free as we can possibly get it. There are networks around and techniques which will allow for essentially error-free communication between computers and between people and computers. It wants to be very responsive so you get answers as quickly as possible. It wants to be very robust, and it wants to support transmission at rates that not only people can use but are well matched TV computers as well.

In terms of presentation of information to a human the assimilation rate would be limited by what the human, himself, could comprehend. Machines may need to pass data back and forth at much higher rates. I think some of the comments about optical transmission would be appropriate in that limited context, in particular.

Second, is the computer area. We have seen not only a rapid growth in the capability of machines, themselves, but also in terms of their architectures, languages that run on them, operating systems, data bases that can work on multiple machines, distributed processing techniques, large address spaces to handle very large programs, etc. We are also seeing the use of these machines in a number of modes of operation which I would call intelligent. That is the third bullet on the slide.

Artificial intelligence is a new discipline which has emerged over the last two decades. It has as a major goal to understand how to make machines behave in ways that human beings would call intelligent if another human being could do the same thing. As a result of that, we believe that the technology is now at a point where it is possible to use machines to do tasks that were previously people-intensive, that required real experts in the field. You can now expect machines to assist in planning, replanning, to prepare situation assessments, to aid in the filtering of crucial data in information overload situations, that even 5 to 10 years ago would not have been believable. We don't have many systems like that today, but we can point to a few intelligent systems. The command and control area is a particularly important one where such progress has been achieved, and emergency management is very similar to command and control.

I think artificial intelligence applications offer tremendous prospects for being able to use computer communications in ways that were impossible to envision being realized in any finite time frame, even 5 or 10 years ago.

Mr. GORE. Are you talking about VHSI technology, or are you anticipating the so-called fifth generation?

Mr. KAHN. Neither really. Artificial intelligence involves a conceptual approach to the organization of programs and software that allow machines to process data symbolically rather than in

the normal number-crunching sense. It is where you can take information and store it in knowledge bases that contain more than just the raw data.

For example, if you are dealing with the Pearl Harbor complex that Dr. Belden talked about, it is one thing to say there are Japanese ships in the Pacific Ocean at such-and-such a location, or there are American ships in such-and-such port, but it would be much more useful to know that there is a potential threat on those ships. That is a piece of information that could be inferred by a human, but a conventional data base system probably would not have it in it.

To take a more limited context, suppose you were trying to capture the state of a chess game in a data base. One model of that would be to keep track of the location of all the pieces and all the moves that were made in the past. Yet to any seasoned chess player, that is perhaps the least important of the information. What he wants to know is, where are the threats? Where am I vulnerable? What are my strategies? What is in motion, and so forth? That is the difference between a data base and a knowledge base, and it is largely independent of the underlying computer technology that is used to implement that.

Mr. GORE. It is a software problem?

Mr. KAHN. It is a very advanced kind of thinking about software and organization of problem-solving strategies. It could be implemented directly in VLSI, but seems to be done more in software than VLSI.

Finally, there is the security technology area, which in some cases will become crucial. In particular, I mentioned the terrorist threat earlier. I believe in dealing effectively with terrorist threats, security may be the most critical item, whereas in some of the natural disasters or civil kinds of actions, having nonsecure facilities, in fact, might be an asset rather than the other way around, because you really do want to communicate lots of information to lots of people, so there is that dichotomy between keeping tight control of the information that relates to specific actions and being able at the same time to keep a large number of people commonly informed about what is going on.

[Slide entitled "Information Processing Technology for Emergency Management" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

COMMUNICATIONS

- | | | |
|-----------------------|---|-------------------------|
| ● EXISTING NETWORKS | } | CONVENTIONAL TECHNOLOGY |
| ● MOBILE RADIO | | |
| ● SATELLITE | | |
| ● PACKET RADIO | } | EMERGING TECHNOLOGY |
| ● MULTIPLE SATELLITES | | |

Mr. KAHN. In the communications area there are really three kinds of technologies that I want to talk about today that are conventional: the use of existing networks, in particular, the telephone systems, the existing carrier networks, the value-added networks. These are all available services that could be used. Mobile radio has been in existence for a long time and will continue to find utility in this arena, particularly for voice communication. The walkie-talkie is of that form. And satellite communications has become widely available for use in point-to-point communications, wide band and long-haul particularly.

I want to discuss two kinds of emerging communication technologies which I think can make a significant difference.

One may be applicable in the short term of the next 2 or 3 years, perhaps, and the other one possibly by the end of the decade. They are both technologies that are based on the notion of packet switching which may be familiar to the subcommittee, but I thought just in the interest of the record, I would say a few words about what that is.

Packet switching is a kind of communications switching technique that differs from conventional circuit switching in the sense that you don't set up point-to-point circuits between the senders and the receivers of data. Rather, it involves a network concept for using many communication channels of various kinds, whether they be satellite links or ground radio links, or point-to-point circuits of various kinds. Those channels are linked together through minicomputers or microprocessors, such that data which travels on any one of those channels can be rerouted down other channels by choice of the minicomputer. The data that flows through the network is organized in the form of packets of information.

A packet is typically a small number of bits of data, typically what you might type in a little message or a short command of some sort, or a little piece of a larger file. There are very few interactions between computers that are of the form of long streams of data. And even when you are trying to transmit long files which you might visualize having that form, the computers will generally break them up into finite size blocks and send them block after block, at which point they are put together at the far end and reorganized into a big sequential file.

The advantage of packet switching is that you don't rely on a full end-to-end circuit between the sender and receiver being setup or operational in order for end-to-end communication to take place. It may be that there is no path between New York and San Francisco, but you do have a path between New York and Washington right then, so you can get a little bit of data to Washington, and then moments later there is a path between Washington and St. Louis, and so it can go there.

Shortly after that, there is another path down to Albuquerque, and shortly after that, one up to San Francisco. This technique may introduce a very small amount of delay in the communication in an emergency situation (typically a fraction of a second), but it can also guarantee that in some cases the data that was transmitted can, in fact, reach the destination despite the fact that a direct path was not available. It is also a very cost effective communications alternative.

An analogy might be in the difference between traveling over a fixed railroad track between one place and another and traveling by car over a road system where if there is a difficulty on one road, you can take some other road, reroute yourself. That discrete entity, the car (like the packet), can make it to the destination where, if there is a difficulty at any portion of the track then the train is essentially unable to proceed. One could build complex switching systems of railroad tracks to follow that analogy further, but then it would begin to make the train system look very much more like a packet switched network, particularly if the trains were very small and compact.

There is an inherent advantage in this kind of network in an emergency situation, where facilities may be subject to attack, either by terrorist groups or just normal kinds of failures. It is a particularly attractive kind of system in the military context, and I think it would have application as well in the civilian domain.

One example of such a technology is packet radio. There are currently several commercial networks that use packet switching on wire line systems, but packet radio applies this concept to the notion of broadcast radio.

[Picture shown.]

Mr. KAHN. This is a picture of a packet radio which we developed at the Defense Advanced Research Projects Agency. It is about a cubic foot in volume. It weighs about 40 pounds, so you can actually carry it in your hands. This is a prototype of a packet radio with a microcomputer controller shown on the bottom, which totally controls the radio. It takes in data and stores it in this microprocessor. It controls the radio portion shown on the top, which is a spread-spectrum radio. The radio can broadcast a packet

of information at any time the microprocessor chooses. Typically, the radio will listen on the air and when the airways are quiet, it will broadcast it.

You can have many of these radios organized together to form a network in some urban or rural area and the radios will all interoperate with each other in the same kind of way a network of people might operate. Namely, one person would talk, someone might hear him, one would relay it on and so on. It might go hundreds of miles using packet radios that way.

One reason this technology is so attractive, is that it's a completely portable kind of technology. It requires very little time to set up. These are the first of the prototype units we have ever built. Within the next few years we project they will be essentially pocket size and will enable computer communication to be established in virtually any needed setting.

So this is, in fact, the kind of technology which would support the introduction of the most powerful of modern computing into virtually any emergency management situation. It is especially useful in situations which involve portability, mobility, and reacting to situations over geographic terrain where advanced plans are not available, and where there are no fixed communication installations.

The packet radio technology is a completely self-organizing kind of system. The packet those radios could be on trucks or in jeeps, in people's hands; the whole system can be in motion, and it will completely organize itself, self-adapt. As long as there is any electronic path to get information from a source to a destination, it will deliver the data at data rates of many tens of kilobits per second, which is adequate for computer communication in this kind of environment.

The second bullet under emerging technology is further off, but we have done enough investigation to believe that it is feasible to embed this kind of technology into very inexpensive satellites. Satellite technology costs on the order of tens of millions of dollars for a typical commercial geosynchronous satellite. Probably we can build some for a few million dollars, depending on the kind of application. Our investigations, however, have led us to believe it is possible to build satellites that might cost on the order of a few hundred thousand dollars in quantities of 100-1,000, to put them into orbit linked together by this packet radio architecture for computer communication purposes. This kind of multiple satellite system would be tremendously valuable in augmenting the kind of capabilities that could be provided by other local distribution systems, for providing rapid response long-haul communication in the kind of evolving emergency situations that we would expect to deal with.

Those are the only comments I am going to make about communication networks per se. It is clearly an important topic. There are other higher level communication issues I am going to come to on the next chart.

[Chart entitled "Interoperability" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

INTEROPERABILITY

- INTERNETWORKING
- MESSAGE TECHNOLOGY
- RECONSTITUTION

Mr. KAHN. If we have the ability to deploy sophisticated networks, the very first question that arises is, how to make these networks interoperate with each other and with other networks that might exist. These could be existing commercial nets or other temporary networks set up elsewhere.

In fact, if you have a crisis situation that involves activity in multiple but rather disjointed areas, you definitely want the ability to set up separate nets, and then get them interconnected, and you would like to be able to use any medium that is available to do that. So the technology for interconnection becomes critical. This internetting technology is now in hand, and I think could be brought to bear directly.

The most critical application for a computer-based system initially will undoubtedly be its use for communicating messages electronically. Electronic mail is a subject that has come up recently in the context of the Postal Service and a variety of commercial networks that are offering it. We have used electronic mail and message systems daily now for over 10 years, and they have become a crucial part of our ability to communicate, especially with large numbers of people. Electronic mail has the property that you can communicate on a point-to-point basis whenever you can get to the person, with deferred delivery or quasi-instantly; you can also communicate with a large number of people simultaneously (in the following sense). A single message that gets typed or otherwise entered into a message system might contain a plan of action that can be communicated within fractions of a second, to

dozens if not hundreds or thousands of electronic mailboxes to be read by other people who might be crucial to carrying out those actions. These messages can be read at any time after they are delivered. The capability may be viewed as an overlay on top of these computer communication networks.

Finally, I should mention the area of communications reconstitution. This is an important aspect especially in the case of terrorist activities which might attempt to destroy various communication resources. A network such as packet radio is inherently very robust, because of the dynamic and adaptive routing which occurs within the net. If you lose even large numbers of radios but still have connectivity from one place to another, the network will alternate-route that data. So the loss of critical components in the net becomes a matter of possibly increased delay or lower throughput, but not loss of connectivity.

One has to deal with the same kind of problem at the more global level of interconnected networks. I think that is a technology we are now beginning to get our hands around.

Each of these subjects come up in the military context, and implicit in what I am saying is that the civilian counterpart of this problem is very similar to the military command and control problem. Much of the technology which would be applicable in the C³ domain could, in fact, be carried over almost directly into the civilian counterpart.

[Chart entitled "Planning/Replanning Aids" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

PLANNING/REPLANNING AIDS

- EXPERT SYSTEMS
- KNOWLEDGE BASES
- GRAPHIC PRESENTATION SYSTEMS
- VOICE INPUT/OUTPUT

Mr. KAHN. I mentioned the use of artificial intelligence technology earlier. The most significant aspect of that use, I think, would be in the form of a variety of expert systems which could be developed. These would be systems which would either possess a lot of expertise, themselves, about some area or would have certain capabilities of logical thinking, such as the ability to plan, if only they had access to the relevant data that could enable plans to be put together on the fly. Plans could be generated which were reasonably accurate and directly relevant to the problem under consideration. Instead of having to anticipate all the contingencies and all of the emergencies with which one might have to deal, the use of an expert system would allow plans to be created at the moment in response to specific events or other inputs.

Planning has historically been a very lengthy process. If one could build expert planning systems, I think one could react to crises and develop very effective plans, or ones which would be at least modifiable to very effective plans, in a very short time.

An expert system derives its expertise on the basis of available information that it can process. It is not just a symbolic inference engine that makes up an expert system. It is all of the expertise about the area that you are dealing with that makes it an expert system.

For example, in the case of an earthquake, you might want to know about the fault system and the road structure. You probably

would like to know about the geographic location of homes, of critical facilities and resources relative to the geography. You would like to know about various kinds of communication in the area. Once that information is accessible, one can reason about it and put together plans.

The last two bullets on that chart are really not so much artificial intelligence as they are augmentations of that capability which will greatly facilitate people's use of the system. The ability to present information graphically can often convey in a very small period of time what it would take reams of paper to convey. Furthermore, the difficulty in making that happen really turns out to be kind of an artificial intelligence problem. If you knew exactly what it was you wanted to display, a priori, you could program that in, but more often than not, you have to decide what it is that is important to present, and that, itself, is a decisionmaking problem of some proportion.

Finally, in many cases it is just not practical to take conventional terminals with you to various destinations; it might even be very desirable to communicate with the system with some form of voice input and possibly even voice output in some cases.

[Chart entitled "Success Factors" follows:]

INFORMATION PROCESSING TECHNOLOGY FOR EMERGENCY MANAGEMENT

SUCCESS FACTORS

- USABILITY
- DEPENDABILITY
- UBIQUITY
- INTEROPERABILITY
- SECURITY

Mr. KAHN. This is my last slide.

In order for this kind of technology to be really usable, it has to be in almost daily use so that people become familiar with it. They should not have to learn to use it at the moment of crisis, it should be a natural part of their normal working environment.

It would certainly have to be dependable to rely on it working in a crisis, but, more importantly, it would have to be ubiquitous in the sense if you needed to get to someone, you would need to know they were likely to be on that system, that they were reachable, that they were able to participate.

The system would have to be made interoperable with other systems of such rules is an important attribute to keep in mind. Finally, for certain applications, it is probably important to provide some means of security within the system so that it cannot be disrupted by hostile elements from outside that system.

That is only a capsule summary of some of the most critical technologies. I would be very happy to go into any one of them in more detail or to discuss the utility in more detail, but I think in the interest of time, I will stop here and ask if you have any questions.

Mr. GORE. What is the practical use in the emergency management of the packet radio system you describe? Give me a scenario.

Mr. KAHN. Well, I think the most immediate thing that comes to mind is that it is the glue that will be able to link distributed people and computers all together, and it can be deployed in a very rapid fashion. If you have to respond to a crisis somewhere, and you need to set up a communications facility quickly, you can do it with this technology.

Mr. GORE. What would you have to have in place ahead of time in order for it to work, a satellite?

Mr. KAHN. You have to have nothing in place. That is the beauty of it. If you were prepared to deploy it in advance—by that I mean you have the equipment at hand and you have all the supportive facilities that you need such as transportation—it probably is fair to say that it could be put into place within at most a few hours and perhaps in as little as a half an hour with the right personnel, from scratch. It is particularly well-suited to handling computer-to-computer traffic. This is not intended as a voice system.

Mr. GORE. Suppose you wanted to put a computer terminal in place at the base of Mount St. Helens, and you wanted that computer to communicate with one in Washington, D.C.

Mr. KAHN. Then that becomes an interoperability problem. What you would probably do is—I am not too familiar with the exact geography out there, but let's assume you could get to Portland or one of the nearby large cities—Seattle—fairly quickly. So what you would do is, you would string a set of these radios—they have a range of some 25 miles or so—string a set of them up and the traffic would then be relayed to some major city, and it could then be interconnected with some other network, whether it is a point-to-point circuit back, or whatever. It provides you the difficult connectivity in those areas where there are not normally facilities available. You could, also, put a satellite terminal right at the base of Mount St. Helens in which case you wouldn't need the radio technology. You could also put the satellite terminal at any intermediate point and use packet radio to relay it back there. But packet radio is more than just a system for relaying traffic to another network or satellite terminal, it can also be used to communicate between many people in a local area such as near the base of Mount St. Helens.

Mr. GORE. Is this system possible to use as a backup for systems vulnerable to EMP?

Mr. KAHN. This particular technology has not been built for EMP, particularly. However, it has the interesting attribute that it does dynamic routing around failed units. If the effect of the EMP were limited to some geographic area and you had packet radios that covered not only that area but the surrounding areas as well, then the system would automatically and dynamically adapt the routing of traffic around the affected area so that communication could still be maintained.

Mr. GORE. Your testimony has been excellent, and I wish we could spend more time on questions, but we have fallen way behind schedule, and we are simply going to have to move forward.

Thank you so much for spending as much time as you obviously did in preparing your testimony. I appreciate it very much. An excellent presentation.

Our next witness is Maj. Gen. Charles Ott, Jr., director of the Arizona Division of Emergency Services and president-elect of the National Emergency Management Association. He will be accompanied by his technical adviser for the Arizona project, Milton Deeever, who is president of the Comtech Data Corp.

I would like to welcome both of you here. We are very glad to have your assistance during this proceeding and, General Ott, please proceed.

[The biographical sketches of General Ott and Mr. Deeever follow:]



Charles A. Ott, Jr.
Director, Division of
Emergency Services



BIOGRAPHY

Department of Emergency
and Military Affairs
State of Arizona

Charles A. Ott, Jr. was born in Santa Barbara, California on September 26, 1920 where he received his early schooling preparatory to entering Stanford University. On graduation, with a B.A. in Economics, he also received an honor graduate commission in the United States Army and entered military service on October 30, 1941.

He served in Europe during World War II with the 76th Field Artillery Battalion and Headquarters, 18th Field Artillery Group. His service took him from the Normandy beachhead through France, Belgium, Germany and into Czechoslovakia. His assignments included Battery Commander, Battalion Operations Officer, Executive Officer and Adjutant and Group Operations Officer. He was decorated for his actions during the German breakthrough and subsequent allied crossings at Remagen on the Rhine River and during the Battle of the Bulge. Following the war he was assigned to the staff of the Sixth Army Headquarters in San Francisco.

In 1946 he resigned his regular commission to enter business in Santa Barbara. He served in a variety of management positions in merchandising, contracting, construction and property development. His service was with essentially family held California Corporations and included Presidencies of both Sterling Supply Corporation and Channel Properties, Inc. Concurrently, he served as a Director of the General Telephone Company of California, the Citizens Savings and Loan Association, and on the Advisory Board of the Crocker-Citizens National Bank in Santa Barbara.

Active in civic affairs, he was President of the Board of Trustees of the Santa Barbara Cottage Hospital, is a past President of the Santa Barbara Rotary Club, Valley Club of Montecito, the Santa Barbara Club, Board of Trustees of the Laguna Blanca School and the Santa Barbara-Ventura Chapter of the Association of the U.S. Army. He was also a Vice President of the local Y.M.C.A. and the Music Academy of the West. He was director of the local Chamber of Commerce and Convention Bureau, Better Business Bureau and the Citizens Planning Association and a member of the U.S. and California Chambers of Commerce, National Association of Plumbing, Heating and Electrical Contractors, Pacific Southwest and National Hardware Associations, National Rifle Association and other business and professional societies.

His military career continued as a parallel to his business and civic activities. He was promoted to the rank of Brigadier General on September 1, 1952 and subsequently served as Commanding General, Division Artillery and Assistant Division Commander, 40th Armored Division, California National Guard. On July 22, 1960, General Ott was appointed Commanding General of the Division and promoted to the rank of Major General. Subsequently, he served as Commander, Southern Emergency Operations Headquarters, and on April 1, 1971 was assigned as Deputy Commanding General, State Military Forces, California.

General Ott was selected as Director, Army National Guard, National Guard Bureau, for a four year active duty tour, Washington, D.C., by the Secretary of the Army and the President and assumed that office on August 16, 1974. He served in that capacity through August 15, 1978. On August 21, 1978, he was appointed Director, Division of Emergency Services, State of Arizona by Governor Bruce Babbitt.

He is currently president-elect of the National Emergency Management Association and will serve as President for 1981-82. He is a member of the Scottsdale Rotary Club and is serving on several advisory commissions related to emergency management.

Personal Data:

Date and Place of Birth: September 26, 1920 in Santa Barbara, California

Parents: Father: Charles Adam Ott, deceased
Mother: Leona Elizabeth Thoete, Santa Barbara, California

Family: Wife: Patricia Jane Parrish Ott
Children: Three - Lesley Jane Thorne, Chris, Mila Lee Tewell

Residence: 5922 E. Calle Tuberia, Phoenix, Arizona 85015
Phone: 946-9808 (home) 273-9880 (office)

In addition to his formal civilian education and senior military college instruction, General Ott attended special courses in nuclear weapons, air defense, maintenance and equipment management, chemical and biological agents, civil disturbance and riot control.

General Ott's military decorations include the Distinguished Service Medal, Legion of Merit, Bronze Star Medal, Meritorious Service Medal, Air Medal, Army Commendation Medal, two Presidential Unit Citations, and Belgian Croix de Guerre. He holds the European-African-Middle Eastern Campaign Medal with four battle stars and the Korean Service Medal with two battle stars.

His military society affiliations include being a Regional President and a member of the Board of Directors of the Association of the U.S. Army. He was a member of the Secretary of Defense Reserve Forces Policy Board from 1963-1967, and the Army Affairs Council of the Department of the Army. He is a member of the American Legion, the Military Order of the World Wars, the Reserve Officers Association, and the National Guard Association of the United States (was National Secretary from 1963-1972).

DEEVER, MILTON L.
President

DEEVER

EDUCATION:

BSEE (with honors), University of California at Berkeley,
1958
MSEE, University of California at Los Angeles, 1962

PROFESSIONAL AFFILIATIONS:

Comtech Data Corporation	April 1978 - Present
Comtech Telecommunications Corp.	June 1976 - March 1978
Motorola	1958 - June 1976

Mr. Deever is now the president, and a founder of Comtech Data Corporation, a wholly owned subsidiary of Comtech Telecommunications Corp. This organization was established to address signal processing in communication applications that is heavily digital-technique oriented.

At Comtech Telecommunications Corp., Mr. Deever, as vice president, New Business Development, was responsible for the definition of new product areas, and the development of new application markets for Comtech's line of advanced communication equipment and systems. As such, he implemented the planning necessary to effect cohesive programs for the design, development, and marketing of resulting products and systems.

At Motorola, Mr. Deever most recently held the post of Director of Planning for the Government Electronics Division. In this capacity he was directly responsible for the organization and operation of the Division's planning efforts including the development of objectives and goals, long-range forecasting, and business analysis. In addition, he was responsible for the direction of the Division's Management Information Systems activity and jointly managed the regional Western Area Computer Center used by both the Government Electronics and the Semiconductor Products Division of Motorola.

Prior to his assignment as Director of Planning, Mr. Deever held several significant position for Motorola starting in 1958 when he joined the company as an Electronic Development Engineer at the Systems Research Laboratory. In this position he was responsible for system logic and circuit design for ground and airborne radar video data processing systems.

In 1961 he was named Regional Marketing Representative for the Government Electronics Division of Motorola and provided representation to Division customers including Boeing, Philco, Lockheed, North American Rockwell, and the NASA Jet Propulsion Laboratory.

He returned to the Systems Research Laboratory in 1962 for a brief assignment in the acquisition of ECM business, coordination of market planning and to lead proposal efforts. He was later reassigned to the Government Electronics Division headquarters in Scottsdale, Arizona, where he held a number of major posts including Program Manager for the Apollo Spacecraft Digital Test Command System (DTCS), Program Manager for the Space-Ground Link System (SGLS) for the Air Force Space Program, and Manager of the Advanced Technology Program Office.

In 1970 he was promoted to Manager of the Communications Operations Marketing Department. In this post he was responsible for the acquisition of new business in space, ground-to-air, satellite, and secure communications. He held the post until February of 1972 when he assumed the broader-scope responsibilities of Director of Planning.

STATEMENT OF MAJ. GEN. CHARLES A. OTT, JR., DIRECTOR,
DIVISION OF EMERGENCY SERVICES, DEPARTMENT OF
EMERGENCY AND MILITARY AFFAIRS, STATE OF ARIZONA,
ACCOMPANIED BY MILTON L. DEEVER, PRESIDENT, COM-
TECH DATA CORP.

General OTT. I am Charles Ott, State director of emergency services for the State of Arizona. I am delighted to be here. I hope I will be one of your catchup witnesses as far as time is concerned.

I just spent four very profitable and enjoyable days in your home State in Nashville, where we had our National Emergency Management Association conference, and I think it is very apropos I should be testifying for you after spending those four delightful days. We have a great many friends there.

Mr. GORE. I appreciate that. I was invited to speak at that gathering, myself. This proceeding was one of the reasons I couldn't. I am glad we got together here.

General OTT. We intend to extend you another invitation.

I have Mr. Deever with me. Mr. Deever—I appreciate the context that he is my adviser. He actually is the president of the corporation which was the low bidder on our satellite communications system which we are in the process of installing. He was working out of his New York offices, and I asked him to come here because the system is a very interesting one, and while I will make a brief introductory statement, I am sure some of the questions that might come to mind would be questions he could more appropriately answer than I can.

The Arizona Division of Emergency Services has designed and is implementing a program which will result in one of the most functional and sophisticated emergency management communications systems in the United States and the only dedicated State emergency management satellite system in the country.

This State-run program was started in 1978 when a comprehensive contract study confirmed what had been obvious for some time: that the State emergency operations center and local government emergency communications capability was inadequate. Communications equipment in the State EOC consisted of loaned, home built, old, and essentially military surplus items that provided very little flexibility for interface with other state agency communication nets. The State and county emergency operations center relied almost exclusively on commercial telephone systems, and had limited access to high frequency and citizens band radio for backup communications. Three presidentially declared flood emergencies in 1978 and 1980 demonstrated that the existing communications system simply could not support major emergency operations.

The 1978 study further revealed that Arizona, like other Western States, faced peculiar problems in emergency communications. These problems relate to physical size of the State, varying terrain features, isolated population centers, rapid population growth and, in many instances, very limited commercial communications facilities. The study further revealed that "piggy-backing" emergency communications requirements onto existing State systems was not a feasible alternative due to the overuse of those microwave systems. To gain a better perspective of the situation that the State

faced, enclosure No. 1 summarizes communications capabilities and equipment available to the EOC in 1978.

To overcome these problems, a detailed emergency communication development program was established. This was to be a multiyear-phased program and would encompass upgrading State and local jurisdiction EOCs with new radio equipment, development of mobile van capability, and a statewide satellite system. Enclosure No. 2 is a synopsis of the original satellite proposal.

Gov. Bruce Babbitt and the Arizona State Legislature have fully supported the communications program objectives, and with the aid of Federal matching funds, significant accomplishments have been made toward meeting our program goals. The State EOC now has a comprehensive array of radio equipment which provides communications capabilities in the high frequency, very high frequency, and the ultrahigh frequency radio bands. The satellite system presently has three stations operational—Phoenix, Flagstaff, and Tucson—and additional county terminals are programmed on an incremental basis. Enclosures No. 3 and No. 3A summarize our present radio equipment and capabilities. Basically, we can now reach any part of the State through extensive radio nets, amateur radio—RACES—agency communications systems. Enclosures No. 4 through No. 15 describe and illustrate the various communications equipment currently operational.

In the satellite area we are presently leasing 1 percent of the power of one of the 12 transponders on Western Union's Westar III Satellite. This power provides us with 4-8 voice channels, plus electronic data transmission capability.

We will expand this number of channels as additional power in the satellite becomes available and our requirements increase. This additional power will then enable us to extend our capabilities of both data transmission as well as voice communication. It is in the area of data transmission that an interesting new field of support for emergency management can be developed—floodplain management, earthquake analysis, nuclear preparedness, et cetera.

The mobile satellite antenna to be used in conjunction with our mobile vans will give us the capability of interfacing with the satellite from any place within the State and within the United States where compatible ground terminals are installed.

By interfacing local telephone links to the satellite terminal at any of the terminal sites, we will be able to communicate with any of the local jurisdictions within the State through the county terminals, and they, as well, will be able to intercommunicate with one another.

The satellite provides a dedicated command and control linkage between the Governor and his staff, the State EOC, the county supervisors and administrative officers, and the county emergency services support systems.

The radio communications equipment in our EOC and mobile vans provide complete radio interfacing with the American Red Cross, the Arizona Department of Public Safety, Arizona State Land Department, Arizona Department of Transportation, Arizona Fish and Game Department, Salt River project, and the Palo Verde Nuclear Powerplant. Using encoding devices we can also access the statewide radio relay systems of these agencies.

Utilizing the radio equipment in the vans we have the ability to communicate with local law enforcement, fire departments, medical facilities, search and rescue, and other emergency services support agencies. Using the mobile vans within a local jurisdiction we can provide communications from any place within the State from any of the local jurisdictions directly to the State EOC. By utilizing the phone-patch capability within our system, we can provide a direct local telephone linkage either by radio or by using other existing radio relay systems from any place where we can establish radio communications.

In addition to the State agencies with which we can communicate, we can also establish communications with such Federal agencies as the Department of Agriculture, U.S. Forest Service, U.S. Park Service, the Bureau of Indian Affairs, Federal Bureau of Investigation, and National Weather Service.

In the area of military communications we can establish direct communications with the active military installations and units in the State, the Arizona National Guard, Arizona Civil Air Patrol, and military and civilian commercial and private aircraft. This capability extends statewide and can also be utilized to communicate with military units in adjoining States or anywhere within the United States with units operating in the HF—3-30 MHz—radio frequency spectrum.

Radio equipment in our EOC and mobile vans covers the entire frequency spectrum utilized by amateur radio operators. We can communicate with amateur radio operators throughout the State of Arizona and throughout the United States if necessary. Utilizing phone-patching techniques we can establish radio telephone communications to any location where a participating amateur radio operator has a phone-patch capability.

The communication vans were designed to provide a total communications capability in all of the emergency service and civil defense communication nets.

The vans have been a subject of interest and study by other State and Federal agencies for possible adaptation as prototypes.

Computer Science Corporation—a study group based in Arlington, Va.—has requested details on our van development in their study for a standardized FEMA mobile communication capability.

Although we are pleased with our progress, more needs to be done. The satellite system must be equipped in every county to become completely effective. Although the State EOC is well equipped at this time, there are some additional features still required to make it fully functional under all possible natural emergency or civil defense conditions. Some of the local political jurisdictions have very limited communications assets and very scarce resources for improving their situations.

A program has been developed to overcome the problems of local jurisdictions. It involves a communication package concept at varying levels of capability which is related to a local jurisdiction threat assessment and civil defense mission. The package concept also envisions a transportable unit for short duration use in areas where mobile vans cannot gain access. Enclosure No. 16 illustrates the communications package concept.

Based on our analysis of local funding capability, it is felt that State and Federal financial assistance will be required in some areas in order to meet the communications capability objectives. The cost of improvements to date, and projections of future cost, are surprisingly low in relation to benefits achieved.

When completed, the total State emergency communications system program outlined will have cost less than \$2 million. Of this amount, less than \$600,000 will have come from Federal matching funds. The State of Arizona is very grateful for the manner in which the Federal Government has responded to our requests for funds, and even though we have gone through extensive reviews to insure that all known requirements are in our current projections, there may be additional requirements as internal State communications developments change due to population geographic shifts and new problems in coordination.

This concludes my statement, Mr. Chairman. I have submitted additional information for the record which I believe is before you, and I would be pleased to answer any questions the committee might ask.

Mr. GORE. Without objection, the additional material provided to the subcommittee will be included in the record at this point.

[General Ott's prepared statement with the enclosures referred to, follow:]

State of Arizona
DIVISION OF EMERGENCY SERVICES



**EMERGENCY COMMUNICATIONS
SYSTEMS SUMMARY**

Testimony Before The
**Investigations and Oversight Subcommittee
House Science and Technology Committee**

Presented by
Charles A. Ott, Jr.

**DIRECTOR
DIVISION OF EMERGENCY SERVICES**

September 30, 1981

STATE OF ARIZONA



DIVISION OF EMERGENCY SERVICES

5636 EAST McDOWELL ROAD
PHOENIX, ARIZONA 85008
TEL. (602) 873-8830

September 21, 1981

The Honorable Albert Gore, Chairman
Subcommittee on Investigations and Oversight
House Science and Technology Committee
1131 Longworth House Office Building
Washington, D.C. 20515

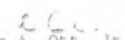
Dear Chairman Gore:

It is my pleasure to transmit herewith information regarding Arizona's emergency management satellite communication system.

One of the cornerstones in the foundation of good emergency management is a reliable, available communication system. Through the use of the equipment described in this summary, we in Arizona feel that we have undertaken the development of such a system. Recent disaster experience shows clearly that the importance of such a positive communication system cannot be overestimated.

I hope this information is useful to the committee in its deliberations. If you have questions regarding this material, please contact me.

Sincerely,


Charles A. Ott, Jr.,
Director

CAO/PFH/jd

INTRODUCTION

The Arizona Division of Emergency Services has designed and is implementing a program which will result in one of the most functional and sophisticated emergency management communications systems in the United States, and the only dedicated state emergency management satellite system in the country.

This state-run program was started in 1978 when a comprehensive contract study confirmed what had been obvious for some time: that the State Emergency Operations Center and local government emergency communications capability was inadequate. Communications equipment in the State EOC consisted of loaned, home built, old, and essentially military surplus items that provided very little flexibility for interface with other state agency communication nets. The state and county Emergency Operations Center relied almost exclusively on commercial telephone systems, and had limited access to high frequency and citizens band radio for back-up communications. Three presidentially declared flood emergencies in 1978 and 1980 demonstrated that the existing communications system simply could not support major emergency operations.

The 1978 study further revealed that Arizona, like other western states, faced peculiar problems in emergency communications. These problems relate to physical size of the state, varying terrain features, isolated population centers, rapid population growth and, in many instances, very limited commercial communications facilities. The study further revealed that "piggy-backing" emergency communications requirements onto existing state systems was not a feasible alternative due to the overuse of those microwave systems. To gain a better perspective of the situation that the state faced, Enclosure #1 summarizes communications capabilities and equipment available to the EOC in 1978.

To overcome these problems, a detailed emergency communication development program was established. This was to be a multiyear-phased program and would encompass upgrading state and local jurisdiction EOC's with new radio equipment, development of mobile van capability, and a statewide satellite system. (Enclosure #2 is a synopsis of the original satellite proposal.)

Governor Bruce Babbitt and the Arizona State Legislature have fully supported the communications program objectives, and with the aid of federal matching funds, significant accomplishments have been made toward meeting our program goals. The State EOC now has a comprehensive array of radio equipment which provides communications capabilities in the high frequency, very high frequency, and the ultra high frequency radio bands. The satellite system presently has three stations operational (Phoenix, Flagstaff and Tucson) and additional county terminals are programmed on an incremental basis. Enclosures #3 and #3A summarize our present radio equipment and capabilities. Basically, we can now reach any part of the state through extensive radio nets, amateur radio (RACES), agency communications systems. Enclosures #4 through #15 describe and illustrate the various communications equipment currently operational.

Although we are pleased with our progress, more needs to be done. The satellite system must be equipped in every county to become completely effective. Although the State EOC is well equipped at this time, there are some additional features still required to make it fully functional under all possible natural emergency or civil defense conditions. Some of the local political jurisdictions have very limited communications assets and very scarce resources for improving their situations.

A program has been developed to overcome the problems of local jurisdictions. It involves a communication package concept at varying levels of capability which is related to a local jurisdiction threat assessment and civil defense mission. The package concept also envisions a transportable unit for short duration use in areas where mobile vans cannot gain access. Enclosure #16 illustrates the communications package concept. Based on our analysis of local funding capability, it is felt that state and federal financial assistance will be required in some areas in order to meet the communications capability objectives. The cost of improvements to date, and projections of future cost, are surprisingly low in relation to benefits achieved. When completed, the total state emergency communications system program outlined will have cost less than two million dollars. Of this amount less than \$600,000 will have come from federal matching funds. The State of Arizona is very grateful for the manner in which the federal government has responded to our requests for funds, and even though we have gone through extensive reviews to insure that all known requirements are in our current projections, there may be additional requirements as internal state communications developments change due to population geographic shifts and new problems in coordination.

In the satellite area we are ^{currently} leasing 1% of the power of the Western Union's Westar III Satellite. This 1% power provides us with 4.4 voice channels.

We will expand this number of channels as additional power in the Satellite becomes available and our requirements increase. This additional power will then enable us to extend our capabilities to ~~transmit~~ data as well as voice communication. It is in this area of data transmission that an interesting new field of support for emergency management can be developed - floodplain management, earthquake analysis, nuclear preparedness, etc..

The mobile satellite antenna to be used in conjunction with our mobile vans will give us the capability of interfacing with the satellite from any place within the State and within the U.S. where compatible ground terminals are installed.

By interfacing local telephone links to the satellite terminal at any of the terminal sites, we will be able to communicate with any of the local jurisdictions within the State through the County terminals, and they, as well, will be able to intercommunicate with one another.

The Satellite provides a dedicated command and control linkage between the Governor and his staff, the State EOC, the County Supervisors and Administrative Officers, and the County Emergency Services Support Systems.

Public Safety Radio Communications:

The radio communications equipment in our EOC and mobile vans provide complete radio interfacing with the American Red Cross, the Arizona Department of Public Safety, Arizona State Land Department, Arizona Department of Transportation, Arizona Fish and Game Department, Salt River Project and the Palo Verde Nuclear Power Plant. Using encoding devices we can also access the statewide radio relay systems of these agencies.

Utilizing the radio equipment in the vans we have the ability to communicate with local law enforcement, Fire Departments, Medical Facilities, Search and Rescue and other Emergency Services Support agencies. Using the mobile vans within a local jurisdiction we can provide communications from any place within the state from any of the local jurisdictions directly to the State EOC. By utilizing the phone patch capability within our system, we can provide a direct local telephone linkage either by radio or by using other existing radio relay systems from any place where we can establish radio communications.

In addition to the State agencies with which we can communicate, we can also establish communications with such Federal agencies as the Department of Agriculture, U.S. Forest Service, U.S. Park Service, the Bureau of Indian Affairs, Federal Bureau of Investigation, and National Weather Service.

Military Communications:

In the area of military communications we can establish direct communications with the active military installations and units in the state, the Arizona National Guard, Arizona Civil Air Patrol and military and civilian commercial and private aircraft. This capability extends statewide and can also be utilized to communicate with military units in adjoining states or anywhere within the U.S. with units operating in the HF (3-30 MHz) radio frequency spectrum.

Amateur Radio:

Radio equipment in our EOC and mobile vans covers the entire frequency spectrum utilized by amateur radio operators. We can communicate with amateur radio operators throughout the State of Arizona and throughout the United States if necessary. Utilizing phone patching techniques we can establish radio telephone communications to any location where a participating amateur radio operator has a phone patch capability.

Communications Vans:

The communication vans were designed to provide a total communications capability in all of the emergency service and civil defense communication nets.

The vans have been a subject of interest and study by other state and Federal agencies for possible adaptation as prototypes.

Computer Science Corporation (a study group based in Arlington, Virginia) has requested details on our van development in their study for a standardized FEMA mobile communication capability.

REPORT TO
STATE OF ARIZONA
DIVISION OF EMERGENCY SERVICES
CONTRACT FOR STATE DISASTER RADIO
COMMUNICATIONS INFORMATION ASSESSMENT PROGRAM

FINAL REPORT
ASSESSMENT, ANALYSIS, SYSTEM LAYOUT
AND RECOMMENDATIONS

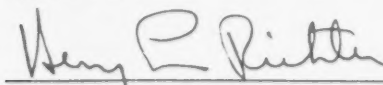
Bernard J. Campbell
Henry L. Richter, Ph.D., Report Editor
Hugh A. Young, P.E., Project Manager

Division of Emergency Services
Purchase Order No. 27, Account Code 26-535-801-00
and
Purchase Order No. 90, Account Code 12-535-030-00

Prepared by:

TeleComm Consultants, Inc.
178 West Longden Avenue
Arcadia, CA 91006

Approved by:



Dr. Henry L. Richter, President

Enclosure 1

EXTRACT

The following is an assessment of the Arizona Division of Emergency Services' (ADES) communications mission capabilities as related to the communications capabilities now in place in the Phoenix Emergency Operations Center (EOC):

The physical facility is a very modern, spacious and well laid out building. The original design seems adequate for development of a disaster communications facility capable of serving the needs of ADES in performing its mission.

TeleComm Consultants, Inc. (TCI) will evaluate the radio equipment from two points of view. First will be its usefulness as an operational radio resource. Second will be its adequacy to perform that function. TCI will also comment on general concepts of communications center installations as they apply to the ADES center.

The comments will be given in sequence following the Radio Services headings in the Emergency Communications Planning Report (CPR), dated August 1977, page 2 ff.

National Guard. Specifically, these comments concern the HF-SSB system operating on 4028.5 kHz-SSB-LSB, segments of which were noted at several county installations throughout the State. TCI must take the position that the kit-built SSB transceivers, even though expertly maintained and modified, do not constitute an adequate equipment base for reliable service in this key role. These units were designed for low budget amateur service which, by definition, implies the presence of an experienced operator. Such an operator will not always be available in disaster operations. As a general statement, any equipment that requires specific operator technical skills should be avoided in an EOC. TCI will detail, in Milestones Two and Three, a professional level system to address the mission previously noted for this system. Specifically, these are a primary military department mutual-aid link between the State EOC, the county EOC's, and the military department monitoring stations. TCI will also specify those features which reflect the state of product developments now available at reasonable prices from several sources. The system proposed by TCI will provide a primary and secondary plan as it concerns the State EOC to county level EOC's. It will also address the limitations and purposes to be served by the use of HF-SSB.

Civil Air Patrol (CAP). TCI noted HF-SSB equipment, on loan from CAP, providing access to the CAP-HF nets. The EOC did not have specific equipment on the CAP VHF, AM (123.10 MHz) net; however, this net frequency is in the ground/air channel assignments, and can be accessed by the transceiver noted in Item 13, page 3, of the CPR. The VHF function of the CAP system is essentially an on-scene resource due to line-of-sight frequencies involved. TCI advises, however, that consideration be given to an installed air/ground capability in the EOC plus the portable unit now on hand. The EOC should not be rendered incapable of air/ground communications when the portable unit is utilized on-scene. TCI was advised that the Arizona Guard helicopters all carry 118 to 130 MHz multichannel VHF-AM capability. This being the case, the above noted requirement becomes even more important.

Department of Public Safety (DPS). TCI is actively pursuing with DPS the options available to implement the primary State-to-county system which will be recommended.

Arizona Land Department. The Arizona Land Department system is terminated in the State EOC. This control station provides entry into the DPS microwave system and through it to 5 mountain-top sites providing coverage to Land Department system users. This is a low band VHF 45.04T MHz 44.76R MHz or simplex 44.76.

Department of Transportation. As now available in the State EOC, the DOT terminal does not meet the more probable need for portability. The 1977 CPR describes the need for a transceiver in the planned Mobile Communications Center. TCI concurs in this; however, comments on the communications requirements in the Mobile Center will be addressed in detail as part of Milestones Two and Three.

Game and Fish. No present access to the Game and Fish system exists in the State EOC. The need is apparent based on the support missions assigned to Game and Fish. While several options exist to establish a point of contact with Game and Fish, TCI will develop its system recommendations based on a capability of direct access from the State EOC and from the Mobile Communications Center. It is not felt that each county EOC will need direct access after the State/county local government system is in place. TCI feels that with reliable State-to-county paths in place backed up by two levels of redundancy (HF and RACES), necessary interchange of Game and Fish information inputs can be accomplished through the State EOC.

Emergency Services State Net. TCI assumes that the net described in Item 7, page 3 of the CPR of August 1977 will utilize frequencies not yet legally available, but under present consideration by the FCC as a Civil Preparedness Radio Service under Part 89 (Public Safety) of the Commission rules. The need for this type of service is clear and has been given support by the national Associated Public-safety Communications Officers (APCO). TCI again emphasizes the comment made in the paragraph headed National Guard regarding operator technical skills.

The Yavapai County Sheriff's net and the net with the Civil Defense nets of Gila and Pinal Counties provide a means of direction and control and mutual-aid from ADES to these three Counties. However, in the final recommendations submitted by TCI, a Statewide capability will be recommended from ADES to each county EOC or other designated point. Standardization and flexibility will be one of the design criteria used by TCI in the process forming the basis for the Milestones Two and Three effort.

Radio Amateur Civil Emergency Services (RACES). TCI has had extensive experience with RACES and other amateur radio group activities. As a result, a policy statement has been developed concerning the organization, structure and governmental involvement which we feel is essential to the use of this resource. Very great variation exists throughout the nation in the capability and record of such groups, and the two articles attached as Appendix A represent the TCI view as to the steps that should be taken by ADES to equip for and organize an effective program to utilize the radio amateur in the Emergency Services Communications role.

The specific equipment observed in the ADES EOC allows such an organization to provide some needed services. TCI suggests that additional VHF-FM (2-meter) equipment be added to prevent a traffic bottleneck now possible. See Appendix A for the paper by Mr. Hugh A. Young and the article by Mr. M. Rosenthal.

Private Radio Services. The Salt River Project Association and the Arizona Public Service systems terminating in the EOC provide unique capability of access to key Arizona quasi-governmental organizations. These will remain important and unaffected by the Statewide Emergency Services net to be detailed. It should be noted, however, that these information sources will be of much enhanced value when ADES has reliable access to each county.

Citizens Band (CB). Many of the comments in the paragraph on RACES and in Appendix A are valid in CB utilization. Legally operated CB is a very limited communications resource, and only if its roles and missions plus effective operator and circuit discipline measures can be defined can it be a meaningful Disaster Services program. TCI agrees, however, that inclusion of CB capability in ADES is essential.

Ground/Air. See notes under Civil Air Patrol as to the need for fixed and portable Ground/Air capability.

Emergency Broadcast System. The remote pickup unit (RPU) located in the State EOC provides the necessary point of input to two key Emergency Broadcast System entry points in the Phoenix area. TCI however, found wide variation in the less developed counties and will comment on these in the county reports. The combination of Telco and RPU access, if properly maintained and exercised, seems adequate.

Civil Defense National Radio System (CDNARS). This Federal system was being upgraded for electromagnetic pulse protection, and provides a very valuable asset in major incident management.

State Emergency Services Communications Net. This urgent need is the prime purpose of the current TCI effort.

SATELLITE COMMUNICATIONS PROPOSAL

INTRODUCTION:

There is a continuing need for communications which can be established quickly and reliably in areas where natural disasters occur such as floods, forest fires, and tornados. These communication systems must be readily transported to the disaster site and made operational within a few hours. The equipment must be entirely self sufficient including primary power source. In general, the equipment would remain at the site until standard communications have been restored which is normally from a few days to one week. Occasionally, the disaster can occur in areas where no communications exist and the equipment may be employed up to one month. This is particularly true for forest fires and is more likely to occur in the Western Rocky Mountain states.

Another essential feature of the emergency communication's system, is that there must be ready access to a disaster headquarters and/or logistics center on an uninterrupted basis. Therefore, point to point communications independent of geographic location, terrain, and weather is a basic requirement of such a system. Simple access to the nationwide phone system is insufficient to meet these requirements as there would be continual delays in routing calls without dedicated lines which must be arranged a priority.

This emergency communication systems requirement can be satisfied employing satellite earth terminals which relay voice and data through a synchronous communication satellite to any point within the U.S.. Many demonstrations have been conducted by groups such as NASA and COMSAT which clearly demonstrate the feasibility of such a communication link. In general, these tests were conducted with experimental satellites of limited operational life or employed relatively large antennas operating through commercial satellites such as WESTAR and SATCOM. A practical economic system dedicated to a particular user has yet to be demonstrated.

A class of satellite earth terminals ideally suited to such an application has been developed. The reliability history of commercial satellites has been outstanding and rental costs for a dedicated satellite channel have been steadily dropping. The capability exists for cost effective "Thin Route Earth Terminal" employing advanced digital voice processing techniques operating on the commercial frequency bands (6 and 4 GHz). The advanced digital voice processing allows more voice channels to be accommodated within a given satellite channel which, therefore, reduces the antenna size and/or transmitter power for a given communication capacity.

Reducing antenna size is essential if easily transportable terminals are to be considered. Disasters which interrupt normal phone service will quite often interrupt normal transportation routes as well. Existing terminals employ antennas ranging from four to fifteen feet in diameter depending on the capacity required and consistent with FCC regulations. A minimum emergency channel would employ a 16 kbs digital voice channel multiplexed with a 100 baud teletype link. A telephone quality voice channel would operate at a 32 kbs data rate and also support three 100 baud teletype channels.

Enclosure 2

Another feature of the terminals is that they can be readily interfaced with a mobile or portable network. A base station can be incorporated with the portable earth terminal at the disaster site allowing relief workers to directly access the satellite link from remote locations.

RECOMMENDED SYSTEM:

A preliminary review of the communications needs for the Department of Emergency Services indicates that a satellite system would be of great value particularly in light of the experiences encountered in the statewide floods of 1978-79. Lack of communications between various flood areas and disaster headquarters in Phoenix was a severe problem as well as poor communications between Phoenix and DES facilities in Flagstaff and Tucson areas.

A dedicated statewide network is recommended which would consist of a master central station at Phoenix employing a fifteen foot antenna and two more fifteen foot terminals which could be installed at Tucson and Flagstaff. As these three stations must be permanently licensed by the FCC, a fifteen foot antenna is required to insure frequency coordination can be readily accommodated with the common carriers in these metropolitan areas. Also, the master control function could then be switched to any of the three locations with minimal modifications to the Flagstaff and Tucson facilities. It is recommended that two types of transportable terminals be considered wherein ease of transport can be traded off against communication capacity. First, a trailer mounted terminal employing a ten foot antenna can be employed when road conditions permit. This type antenna is mounted on the trailer for transport where a maximum width of eight foot is maintained and the trailer can be towed to the site with any general purpose medium duty vehicle. It should be noted that the trailer provides a convenient mount for a base station radio antenna when a portable radio network is incorporated into the system. Up to four voice channels and six teletypes can be linked with a fifteen foot master station with full duplex operation or two telephone voice grade channels and six teletypes can be accommodated by simply switching modes of operation.

For an air transportable system (helicopter or fixed wing) a basic terminal employing a six foot antenna is recommended. The six foot antenna would be divided into two halves which are six feet long, 3 feet wide and 1 foot thick weighing 33 lbs per half section. The other electronic boxes would be less than 9 cu ft apiece and weigh less than 50 lbs each. GEL-CEL battery packs would have to be employed for compliance with air transport rules. Such a terminal could be assembled by one technician and on the air within two hours after arrival at the site.

For each of the satellite channels a discrete frequency is assigned. Such a system is referred to as Frequency Division Multiple Access (FDMA). All traffic is routed through the master station in a "star" network. For each link to the master, two frequencies are assigned for full duplex operation. Once traffic patterns are more accurately known, some channels could be shared on a "demand assigned" basis. This reduces the amount of satellite capacity required and therefore reduces annual rental costs. Annual rental costs are largely based on the amount of satellite power and bandwidth employed for a private network.

Connecting into an existing telephone or teletype network at a fixed station is readily accomplished with existing peripherals. Automatic dialing and signalling can be incorporated into all terminals if required.

FIXED BASE STATION:

The base station equipment recommended for the fixed sites would employ a 4.5 meter (15 foot) antenna especially developed for domestic satellite systems and FCC regulations. This antenna is made from fiberglass which is lighter weight and less costly than aluminum dishes with excellent weather resistance. All equipment not mounted with the antenna can be installed up to 1000 feet from the antenna. It is recommended that a basic prime power of 24 VDC be provided by batteries that are on continual charge so that many hours of operation would be permitted in the event AC power is lost.

The master control station would employ a 75 watt traveling wave tube amplifier for the basic transmitter. The master station must be able to accommodate up to 5 separate frequency channels simultaneously and therefore must be operating in the linear mode. All stations must be fully synthesized to operate over a full transponder bandwidth of 36 MHz. If a transportable terminal is located where it is interfering with local terrestrial microwave or it is being interfered with, then rapid switching to a new channel may be required.

LAND MOBILE STATION:

This station would have a 10 foot antenna mounted on a trailer. The antenna with feed and antenna electronics in place would be mounted on a trailer. The elevation angle of the antenna should be mounted within 4° of the required angle anywhere within the state of Arizona minimizing the amount of elevation adjustment required at an emergency site. The trailer could be parked within 4° of the required azimuth angle and therefore only vernier antenna mount adjustments would be required to locate the satellite. A canvas shroud should cover the antenna during transport.

A five watt solid state transmitter could be employed for this station as only one transmit carrier is required. The baseband equipment could be mounted in a general purpose communications van which also could be used to pull the trailer. The trailer with antenna, antenna mounted electronics, and trailer should weigh less than 1500 pounds.

AIR TRANSPORTABLE STATION:

This station should be identical to the land mobile station except that a free standing six foot antenna would be employed. The antenna assembly should consist of a number of subassemblies that can be quickly assembled on site. The dish should be in two pieces $6' \times 3' \times 1'$, there would be a waveguide feed assembly, antenna mount kit, and antenna mounted electronics box. This antenna could be assembled and aligned by one experienced technician. The baseband unit, cables, and power supply would make up the balance of the system. No assembly should weigh more than 50 pounds, and should be installed in special containers for rough handling in transit.

PROGRAM PLAN:

As this type of dedicated network has not yet been implemented in the U.S., it is recommended that a two step program be considered. The first phase would be to install a master station in Phoenix operating against a land mobile terminal. In the second phase the two additional fixed stations would be procured along with the air transportable terminal.

This two phase program is recommended to minimize economic investment in a new technology. Operating a minimal system for a trial period will more clearly define the niche that can be filled in a statewide communication network by satellite earth terminals.

PHASE I:

The objectives of this phase should be as follows:

1. Gain operational experience with an emergency satellite communication system by DES personnel.
2. Establish definitive rules with the FCC for this class of service in the Arizona area.
3. Establish procedures and tariffs for occasional use satellite channels with Western Union or RCA. To minimize space segment costs, it may be desirable to have a combination of dedicated channels and occasional use channels.
4. Establish a master station in Phoenix and one land mobile terminal for operational use.
5. Determine more accurately the traffic density required for each link; i.e., the best mix of voice and TTY channels.

PHASE II:

This phase would complete a full up system by installing two more fixed stations at Flagstaff and Tucson along with the procurement of an air transportable terminal.

PROGRAM COSTS:

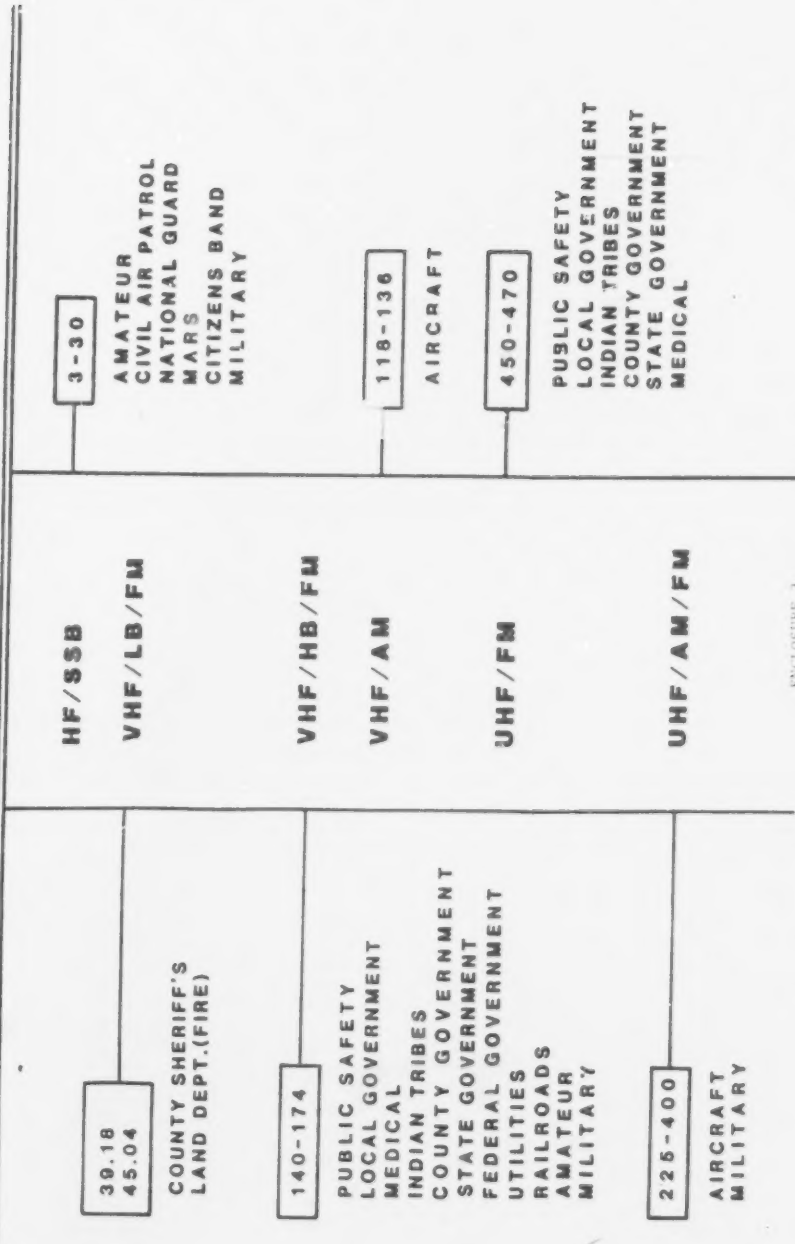
Care must be taken to optimize satellite channel usage for minimum costs. Typically, transponders for private use are rented as increments of 1% of the total transponder power and frequency. Western Union tariffs are approximately \$14K/yr rental fee for 1% of a transponder. Depending on traffic density per channel, size of terminals at each end, and voice quality required, anywhere from 2 to 6 voice channels can be accommodated within 1%.

A private firm must be hired to perform "frequency coordination" for a fixed station in order to apply for a FCC license. These firms have a computer base on file of all existing stations to determine that no interference will occur. Their charges average \$2500 per site to be cleared.

The types of equipment proposed are not currently in full scale production and therefore should be considered as prototype units. Therefore, detailed requirements and specifications would have to be established before accurate pricing could be prepared. For example, the Division of Emergency Services may already own a trailer which could be modified for the land mobile unit rather than procuring a new trailer especially for this program.

The foregoing is a synopsis of a proposal prepared for the Arizona Division of Emergency Services by Motorola.

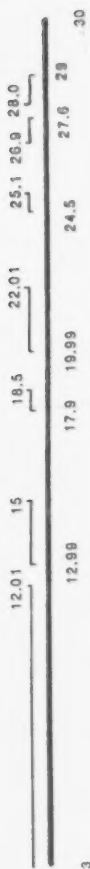
SUPPORT COMMUNICATIONS FREQUENCY SPECTRUM



ENCLOSURE 3

ARIZONA DIVISION OF EMERGENCY SERVICES RADIO FREQUENCY COVERAGE (In Mhz)

HF



VHF



UHF



ENCLOSURE 3A

STATE EMERGENCY OPERATING CENTER
COMMUNICATIONS

CONSOLE 1 Satellite

Console houses inside electronics for satellite system. Provides storage for radio headsets, mics, spare parts and miscellaneous accessories.

CONSOLE 2 Public Safety

GENERAL ELECTRIC HI POWR MASTR EXEC II VHF LO BAND
Crystalled frequencies for American Red Cross and Maricopa County Civil Defense.

GENERAL ELECTRIC HI POWR MASTR EXEC II VHF LO BAND
Crystalled frequencies for Arizona Land Department.

WULFSBERG WMC-100-0. VHF 150-174 MHz
Covering law enforcement and state and local government agencies.

COLLINS VHF 251 116-136 MHz.
Covering aircraft frequencies used by private, commercial and National Guard aircraft.

MOTOROLA SYNTOR UHF 460-465.5 MHz
Covering state and local agencies and law enforcement.

BEARCAT 220 SCANNER
Frequency coverage in VHF and UHF bands.

PIPO TOUCH TONE PAD for accessing repeaters.
COMMUNICATIONS SPECIALIST TONE ENCODER
Used to access repeaters.

VIKING PHONE PATCH
Phone patch facility for patching any radio in console.

CONSOLE 3 Amateur

ICOM 255 2-METER. 144-148 MHz.
Solid-state, fully synthesized with memory and scan functions.

KENWOOD 120S HF SSB. 3-30 MHz
in the designated amateur bands.

COBRA CB Citizens Band Solid-state.
Used in Search and Rescue conducted by county Sheriff's office.

TOUCH TONE & PHONE PATCH.
Full facilities for repeater access and phone patching.

CONSOLE 4 MilitaryNATIONAL GUARD/CAP

SWAN ASTRO 150C HG SSB
Modified to cover Civil Air Patrol and National Guard frequencies.
Solid state and fully synthesized.

KING AIRCRAFT KU-193
4 Channel crystallized.
Used for Air/Ground and Air/Air Civil Air Patrol traffic.

GENAVE VHF 2-Meter
4 Channel crystallized for use on CAP dedicated 2-meter frequencies.

VIKING PHONE PATCH
Phone patch facility for all radios.

COMMUNICATIONS VEHICLE RADIO EQUIPMENT

AEROTRON "COMPANION" VHF/FM TRANSCEIVER

Low band, 5 channel, frequency range 30.0 - 50.0 MHz, RF power output 50 watts, crystallized on 44.76 and 45.04 MHz with the Arizona State Land Department for fire suppression.

COBRA 21 GTL, HF/AM TRANSCEIVER

"Citizen's Band," 40 channel, frequency range 26-27 MHz. CB is utilized by many jurisdictions as supplemental communications in search and rescue efforts.

MOTOROLA SYNCOM-10, VHF/FM TRANSCEIVER

140 - 174 MHz, 2.5 KHz spacing, 9598 channels, fully synthesized, 10 watts with electronic frequency display, reprogrammable electronic memory. Two transceivers are located in the communications van with 75 watt amplifiers. Transceivers have been modified to allow repeater operations in the VHF high band spectrum.

GENERAL ELECTRIC, MASTER EXECUTIVE II, VHF/FM

Low band, transceiver, solid state, 4 channel, frequency range 29.7 - 50.0 MHz, RF power output 100 watts, crystallized on 39.10 and 39.18 MHz allowing voice communications with many counties, small political jurisdictions and some tribes.

MOTOROLA, PET 25A, TRANSCEIVER

VHF (116 - 150 MHz) and UHF (225 - 400 MHz), fully synthesized, solid state, 8260 frequencies, electronic frequency display, electronic memory and scan, AM/FM, and beacon mode. Unit allows voice communications with commercial, private and military aircraft.

KENWOOD, TR-7625, SYNTHESIZED

2-meter amateur FM mobile transceiver. Combined with the Kenwood RM-76 microprocessor control unit, several memory and scanning capabilities are provided by the equipment. Has full 5 KHz coverage from 144.000 to 147.995 MHz, automatic memory scan, digital display of transmit and receive frequencies and operating functions. Multichannel (800 - channel) operations, RF output power: High 10 watts, Low 1 watt.

KENWOOD, TS-120S, SSB/HF, AMATEUR TRANSCEIVER

Frequency Range: 80M Band 3.5 - 4.0 MHz, 40M Band 7.0 - 7.3 MHz, 20M Band 14.0 - 14.35, 15M Band 21.0 - 21.45, 10M Band 28.0 - 29.7 MHz. 200 watts PEP for single sideband operation.

Enclosure 5

SWAN ASTRO 150, SSB/HF, AMATEUR TRANSCEIVER

Frequency Range: 80M Band 3.0 - 4.5 MHz, 40M Band 6.0 - 8.3 MHz, 20M Band 13.8 - 16.0 MHz, 15 Band 20.8 - 23.0 MHz and 10M Band 28.0 - 30.0 MHz
235 watts PEP on all bands. Factory modified for Arizona National Guard, Civil Air Patrol and Arizona MARS HF frequencies.

NYE VIKING PHONE PATCH

Connects a telephone circuit into any transceiver in the van except CB and amateur 2-meter.

COMMUNICATIONS SPECIALISTS TE64 ENCODER

Provides all continuous tone coded squelch frequencies (CTCSS), touch tones, test tones and burst tones necessary for the signaling to repeaters.

BEARCAT 220 CRYSTALLESS SCANNER

Twenty channel capability with microprocessor, keyboard and operation section that controls scan, lockout for unwanted channels, direct channel access, service search, selectable speed control for scan and search, priority and programmed search.

Frequency Coverage: VHF LB 32-50 MHz Governmental Business
VHF 118-135 MHz Aircraft
VHF 144-148 MHz Amateur
VHF HB 148-174 MHz Public Safety
UHF 420.450-470 MHz Public Safety

AG-TRONIC GENERATOR SET

Electronic, gasoline, 4500 continuous duty watts, 120/240 output voltage and 38/19 amps. Unit has remote start and operate controls. Unit supplies 120 volt electronic power to two Hewlett Packard DC power supplies which charges two high ampere hour RU type 12 volt batteries.



LEFT VIEW OF THE EMERGENCY OPERATIONS CENTER COMMUNICATIONS CENTER

The State Domestic Satellite Control Console is shown in the far left of the picture. The two operator consoles shown provide positions for Public Safety (left center) and Amateur Radio (right) Nets. Four operators can be accommodated, and phone patching and automatic frequency scanning capabilities are built into the consoles. Citizen Band radio is also included in the amateur console position. These consoles provide a wide range of capabilities for operations in other state controlled radio nets, and broad coverage in the amateur and citizen band radio frequency spectrum.

ENCLOSURE 6



RIGHT VIEW OF THE EMERGENCY OPERATIONS CENTER COMMUNICATIONS CENTER

The Amateur Console is again shown in the center of the picture. The Military Console (far right) contains radio equipment for communicating with the Arizona Army National Guard, other military units, aircraft, and the Civil Air Patrol. Communications consoles within the communications center provide positions for up to six operators at one time in addition to positions for operators of other equipment located in the communication center.

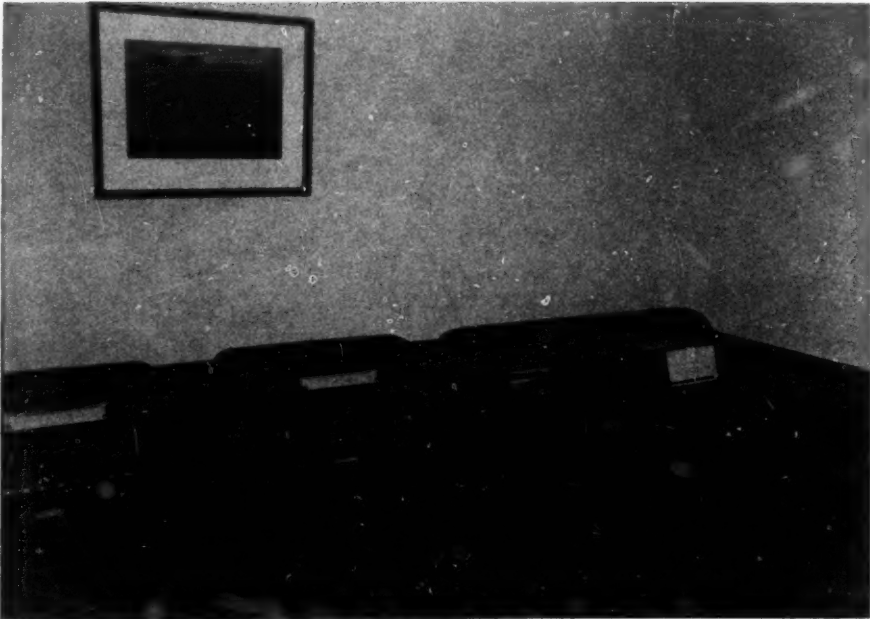
ENCLOSURE 7



CIVIL DEFENSE NATIONAL RADIO SYSTEM
AND EMERGENCY BROADCAST CONSOLE.

The Civil Defense National Radio System provides direct radio (voice and cw), and radio teletype communications with Region IX of the Federal Emergency Management Agency, and is also capable of providing long-range radio and radio-teletype communication to other states and national agencies in the high frequency spectrum range. The Emergency Broadcast Console (lower right front) provides direct voice radio communications with the Arizona EBS control stations.

ENCLOSURE 8



NATIONAL WEATHER SERVICE AND CIVIL DEFENSE NATIONAL TELETYPE SYSTEMS.

The National Weather Service (NWS) teletype receiver (left) provides continuous information regarding local, state, national and international weather conditions and hazard warnings. The Civil Defense National Teletype System (2 equipments on right) provide simultaneous (full duplex) send and receive teletype capability. Messages may be transmitted by keyboard typing or a prepunched tape. The system provides nationwide teletype interconnects.

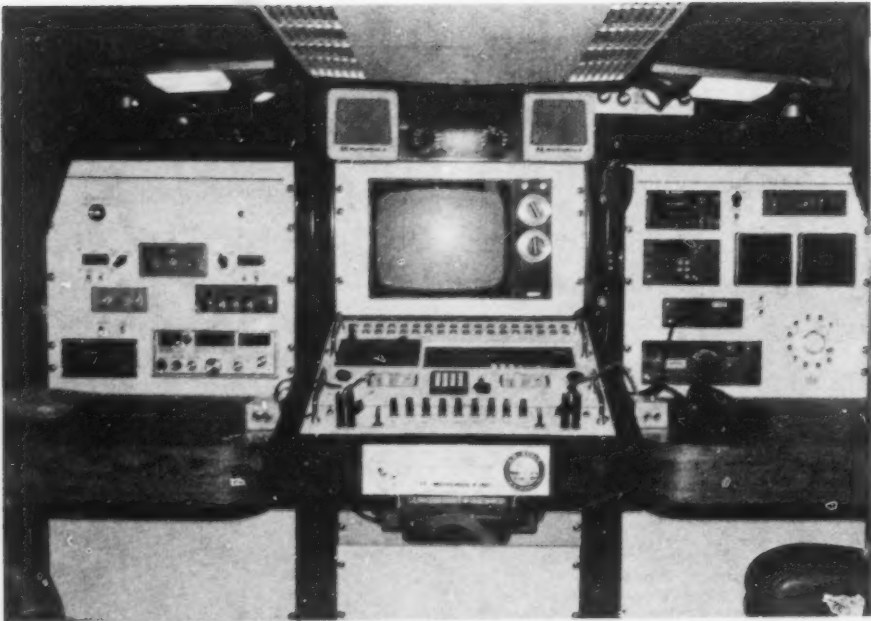
ENCLOSURE 9



MOBILE COMMUNICATIONS VAN, LEFT-SIDE VIEW

The Arizona Division of Emergency Services Mobile Communications Van (one of two), is completely equipped for self-sustained communications operations. The van is equipped with a separate heating/air-conditioning system, extra gas tanks, extra batteries for radio operations, and a portable generator for recharging the radio power supplies. Connections are built in for 110V operation from commercial sources when available. Communications equipment installed in each van provides capabilities similar to those in the state emergency communications center.

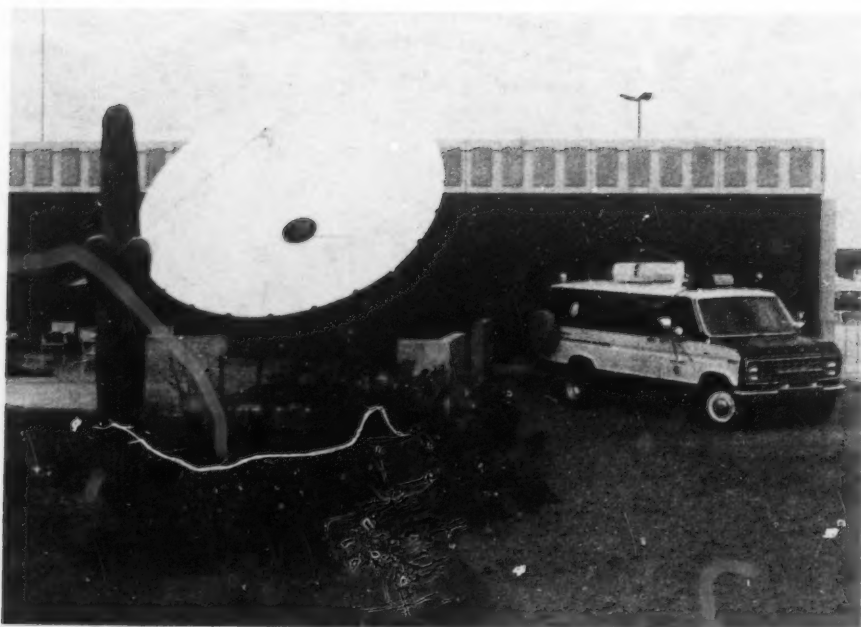
ENCLOSURE 10



MOBILE COMMUNICATIONS VAN OPERATOR CONSOLE

The communications van provides positions for two operators. Installed equipment provides a wide range of capabilities, including interfacing with the State Communications Center, other state agency communication nets, military and amateur radio nets, and phone patching between radio nets and commercial telephone systems. The control panel (center) provides the capability for interfacing different radio nets, and simultaneous monitoring of several other radio nets. The television receiver (upper center) is for monitoring local television transmissions.

ENCLOSURE 11



COMMUNICATIONS VAN, AND SATELLITE ANTENNA

This view shows the communications van previously described, and the domestic satellite antenna dish located at the State Emergency Operations Center prior to completion of the installation of the antenna. The building in the background contains offices for part of the Arizona Military Department and the Arizona Division of Emergency Services. The State Emergency Operations Center is located in the basement level of the building.

ENCLOSURE 12



COMMUNICATIONS VAN, RIGHT SIDE, AND DOMESTIC SATELLITE ANTENNA

Another view of the mobile communications van from the right side. The antenna dish, (right front) is for the control earth station located in the State Emergency Operations Center (EOC). The EOC is located in the basement of the building in the background. The antenna dish is 5 meters in diameter, and is one of 11 presently installed. Ultimately, the state will have one satellite terminal in each county for a total of 14.

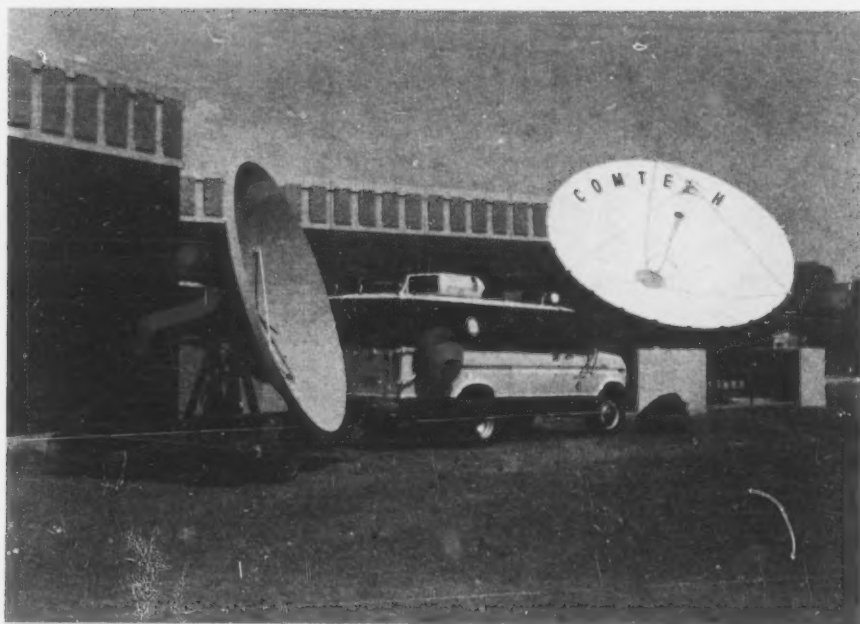
ENCLOSURE 13



COMMUNICATIONS VAN WITH TRANSPORTABLE ANTENNA ATTACHED

The transportable antenna will provide satellite access from remote locations. Because of the satellite location, the portable antenna should not require more than four degrees adjustment in order to focus on the satellite. The antenna shown is a prototype. The antenna that will be available to the Arizona Division of Emergency Services will be a folding type for easier mobility.

ENCLOSURE 14



COMMUNICATIONS VAN, TRANSPORTABLE ANTENNA, AND MAIN EARTH TERMINAL

All of the necessary earth terminal electronics for the portable antenna will be mounted on the trailer with the antenna.

ENCLOSURE 15

Mr. GORE. That is mighty impressive testimony, and the system you have in place is quite impressive. Not least impressive is the cost figure of under \$2 million for this entire setup. That is really something.

Mr. Deever, do you want to add anything to what General Ott has said?

Mr. DEEVER. Only that we have been very happy to work this system because it shows that although satellites were listed in the prior discussion as being existing capability, it is really just coming online as being a normal, functional entity upon which people can draw.

We were very happy to work in this area because we are doing probably as much as is being done anywhere in the satellite side. The kinds of equipment we are using are as advanced as any, and it is not a curiosity; it is being used every day now, and we have essentially checked out every station that we have been able to get online to date, so it is so-called events technology, but it is nuts and bolts as well, because we are currently in use on the system.

Mr. GORE. Do you utilize computer capability in this system now, General?

General OTT. No; we don't, but it is envisioned. I think probably when Jim Morentz comes on a little later on—we have been working with him and his computer program. Our State, not unlike other States, has a State computer system, and we have a linkage to that. However, that is a 40-hour-a-week, 8-hour-a-day system, and with very little persuasion I was able to get the State administrative officer to recognize that emergencies don't usually happen during the middle of an 8-hour workday; they happen in the middle of a Sunday night, when you are sound asleep and the system would not respond.

So we have purchased a small, inexpensive, about a \$15,000 computer system, which we have brought online, and we are now working to interface with the national system that Jim will describe to you. We do have the capability of bringing up immediately our assets resources and various other important matters that are for us a functional requirement in case of an emergency that would happen at any time of the day or night.

I think we will be able to interface this.

I would like to say in the data field we are getting very excited. We worked with the National Weather Service on a trial basis, which we think is going to be installed this year, that has to do with the many floods that we have in Arizona, and it relates to the monitoring devices that I am certain the chairman is familiar with. It is being installed in many of our rivers out there. If we can project the satellite collection of the data and then transmission into existing county emergency operation centers, we can have an instantaneous report into these counties on a readout 5 or 6 hours before the flood crest that is measured would ever reach a particularly highly populated area, and this gives us a very needed early response capability at all levels.

Mr. GORE. That is terrific. What other contingencies might be addressed by this new capability?

General OTT. Earthquakes are certainly one. California is working on one of these systems, and we can tie in very easily with the satellite system.

Nuclear offsite safety is certainly another one. The nuclear—ultimate nuclear attack, of course, would be another one.

Mr. GORE. On oversight safety you have in mind that sensors would read directly into computers that will relay the information in useful form?

General OTT. That is correct, sir.

Mr. DEEVER. I would mention in the satellite system one of the considerations was that it be capable of digital communication, even though the initial requirement was for voice, so the system is a digitized system. It is a digital voice network, and it is at high data rates that you cannot get over normal telephone lines, and with difficulty over microwave. That was one of the basic precepts, that it had to go toward data communication in the long run; so we started with data communication in the first place.

Mr. GORE. How many bits per second?

Mr. DEEVER. Each channel right now is at 37 kilobits for each voice channel, but it is expandable in any way you want. Normally we operate up to 1½ megabits. That is sort of a standard.

Mr. GORE. General, do you make use of networking of key personnel?

General OTT. Yes; Mr. Chairman, we do. As a matter of fact, we go online, when we go online with Palo Verde, which is about 1½ years away, and that will be the largest nuclear power facility in the country, we envision a complete 24-hour operation which links in a series of a half dozen State and county emergency response organizations for instantaneous communication.

One of the things that is interesting to me is, in testimony we had from the legislative representative from the State of Pennsylvania relating to Three Mile Island, was the terrible problem with communication. We will have four basic communication links to the powerplant site, which is 50 miles west of Phoenix. The land-line will be, certainly, one.

The two types of radio, the microwave and the standard radio communication, and then in addition the very important satellite, I think this will give us a unique command and control capability on a satellite which will not interfere with or necessarily become a part of the rather broader spectrum of the other types of communication. This can also be a secure type of communication. We have that capability built into the system.

Mr. GORE. You have projected tests to try out your emergency response system; is that correct?

General OTT. That is correct, sir.

Mr. GORE. Have you had any problem with training the personnel participating in the system?

General OTT. Yes, but it is an ongoing process, and we have been very fortunate because of the number of emergencies we have had in the State that vary from insects to almost anything you might imagine, the Governor and the legislature have provided me with additional exempt positions which permitted me to train these people in advance of their being hired on a permanent basis so we

have a constructively cycled training program going on all the time now.

Mr. GORE. Has the stream of visitors from other States started up yet?

General OTT. I don't think that the temperature has gotten low enough, but we will be there in about 2 weeks. We are up to 100 or 102. When we get to 95, we expect it. FEMA, as we know, has gone through a reorganization process and some of the people that are new onboard there have not yet come out, but we intend to get them there and everybody seems to have shown an interest.

Uniquely, while we like to take credit for all this as being something unusual for our State, we are a relatively new State and having been relatively new there myself, I learned something about the history. There are 14 counties there, even though it is the 6th largest State. When we talk about financing a system to get into each county seat, it is a good deal less expensive and more triable within the realm of our local governments, the State and Federal Governments and our State finances.

Mr. GORE. I guess you are already there.

General OTT. We are getting there. I feel that this whole idea of comprehensive emergency management is just one that we have to address. My background is essentially civilian. I was a National Guard officer, and I had an opportunity to serve on active duty two or three times in various conflicts, but I just feel that the civilian community as well as the private sector, particularly the volunteer agencies, they represent a tremendous potential. I frankly look at the next most important thing we are doing as a training and education program to train all of the citizens, what they can do as far as emergency management is concerned.

Frankly, if everybody was able to do just a little bit, and if we harness this tremendous power of private industry and the voluntary agencies to assist us and get them as part of a team, we are going to be able to attack this thing much better than we are doing right now.

Mr. GORE. If we can make it work, then maybe we can make it work with respect to other challenges facing Government as well. I am encouraged by what Arizona has been able to do. It has been most impressive. Thank you for sharing it with us today.

General OTT. Thank you for inviting us, Mr. Chairman, and we hope to be able to pass on anything we learn from this to you and to your committee.

Mr. GORE. We will look forward to following with interest the progress you all make there. I know that the other 49 States will be following it, too.

Thank you so much for coming today.

Our next witness is Charles K. Allen, director of the department of public affairs and safety in Plainfield, N.J. Mr. Allen, if you will come forward, we are very pleased to have you join us today.

Without objection, your statement will appear in the record, and we would like to hear from you at this point. Thank you for coming.

STATEMENT OF CHARLES K. ALLEN, DIRECTOR, PUBLIC AFFAIRS AND SAFETY, CITY OF PLAINFIELD, N.J.

Mr. ALLEN. I, too, am very honored to be here before this committee. I would like to bring you the situation of emergency management from the viewpoint of a local emergency manager. Heretofore, they may have been known as the civil defense directors. With the reorganization we have been elevated to the rank of emergency managers.

My background essentially is in the area of law enforcement and emergency services. I serve as the director of public safety, which involves the police and fire forces of our community. Plainfield is a city about 25 miles from New York City, occupies 6 square miles, 50,000 people. We are located in one of the most populous counties in New Jersey, namely Union County, with heavy industry, two major airports, and the potential for mass destruction.

My primary concern as a local emergency manager is the protection of life and property. Theoretically, I am to serve in coordinating emergency resources, but in my dual role as director of public safety, I do have the opportunity to impact on how the resources are utilized. I don't have the chain-of-command problem that was mentioned by an earlier speaker. I can issue orders. They are expected to be carried out—although in other municipalities they are civilians and they have pretty much of the policy problems mentioned earlier.

In the city of Plainfield, N.J., as we began our emergency operating plan, we formulated an emergency planning committee. This committee is composed of five personnel, leased personnel, social service agencies, public works people, and each is expected to have an expertise in his particular field at the local level.

We expect that he does have contacts with persons more expert than he on a broader basis, but we tend to plan our emergency responses around a local need. Essentially we are confronted with floods, power outages, and with our ethnic makeup; there have been some social disruptions over the years, a major one being in 1967, which was precipitated by loss of life, but it did result in extensive property damage and even today we feel some of the social effects of that riot some 14 years ago.

As a local emergency manager—and I wish to emphasize that I am speaking from the standpoint of the local emergency manager—during the crisis that we have had over the years, our present communications capability has been adequate. Again, that is for the local need. We have frequencies that are operated by our fire department, our police department. We have one for our public works. We are tied in directly with our local county network. They, in turn, have access to the other counties throughout the State of New Jersey.

In the interest of time, I would like to relate two major incidents that occurred in the last several years and indicate to you how we did respond. There was great local initiative, great local initiative. The people on my emergency operating council are volunteers. They are assigned by their employers, but they are part-time emergency planners. Whenever we anticipate or have word or predict that a crisis will occur—let's stick with a situation such as the riot—I immediately convene this operating council. We will go to

our emergency operating center conveniently located in the basement of the police headquarters. We will critique what we may reasonably anticipate based on the information that we have received to date. Based on that analysis we will determine the extent to which we are going to deploy resources, or even make additional notification.

You heard people earlier talking about having the right to make a mistake. This is very critical. If we cry wolf too early, the next time around we may need the resource, and it will not be available. It is not that we are afraid to make mistakes, but we do know that there are many people always watching, and criticism will not come during the crisis, but you can bet the day after, when things are quiet, the Monday-morning quarterbacks, as they are known, even some in my own profession, are quick to talk about what should have been. So we would like to minimize this in terms of our decisionmaking process; but it is real, and we are very, very cognizant of it.

With the riot early in the game, my recollection and my reading of the history is that we thought we could contain it with local resources. We began to get information that outsiders were involved, and based on that bit of information, we did notify county and State. At this juncture, the State literally took over our city. I submit to you we are still suffering some of the ills of their participation. Well meaning as it was, needed as it was, some of the personnel and some of the tacticians to which they resorted, were quite offensive, even to those who were not participating in the disturbance.

Of course, once it was quelled, they left, and we are there to deal with the problems and their residues.

In the instance of about 6 months ago, as I indicated, we have miles of major highways in our area. A tank truck became wedged under a railroad underpass at the height of the commuter rush. It began to leak a substance whose properties we did not know. The driver of the vehicle was unable to locate his manifest and for several minutes there, we did have a real problem.

We communicated with the trucking company, the manufacturer of the product. They identified a person within 12 miles of the scene. He responded, advised us of the properties and the best way to contain and fight any potential conflagration, and that matter was contained with no loss of life and minimum property damage. In fact, the situation lasted less than 12 hours despite the fact that it received national publicity.

As a local manager, my needs are sufficient warning for impending problems. In my area we have not yet been visited by earthquakes. Floods, yes. Large fires, yes. With the two airports and the transport of many dangerous commodities we need people who can best advise us on the properties of those commodities and the resources that should be brought to bear to contain them.

We communicate on a daily basis with our county net. That agency has extremely competent individuals leading it. They have a massive contact with experts throughout the State who we feel can supply us all the information, and it is my understanding—I must again speak from the standpoint of a local manager—it is my

understanding they have set up a network of communication which can adequately address any emergency.

I would like to share with you, in closing, that I listened with interest to General Ott. I am fascinated by his plan. I brought a bias to this table, or to the chair before coming to the table, that much of what is being talked about in communications and networking, I was under the impression that it was an extremely expensive operation, and I am glad that General Ott put my mind at rest to that extent, and earlier today I was somewhat reluctant to accept it. Based on his presentation, I feel it has a great deal of merit, and he has given me a challenge now to do more review in that area, and perhaps we can recommend it more strongly for our State agencies.

Thank you very much.

[The prepared statement of Mr. Allen follows:]

PREPARED STATEMENT BY CHARLES K. ALLEN

COMMUNICATIONS TECHNOLOGY FROM A LOCAL PERSPECTIVE

I would like to express my appreciation for the invitation to participate in the discussion regarding traditional and advanced networking as it affects the control and management of emergencies at the local (Municipality) level. I wish to bring this Committee the view point of a local emergency manager who is presently serving in that capacity in the City of Plainfield, New Jersey. Our City, which is located in Central New Jersey, has some 46,000 residents and comprises approximately six square miles. It is one of the major urban centers in Central New Jersey and is surrounded by suburban and rural communities. The density of our population is evidenced by the description previously given and the economic status of our citizenry ranges from the very poor to citizens who might be termed "wealthy". We sometimes refer to ourselves as a microcosm of larger urban centers. Plainfield is located in Union County which is one of the more densely populated counties in the State--if not the nation--containing over one-half million persons in approximately one-hundred square miles. Union County is composed of twenty-one communities, two airports, over one hundred twenty miles of railroad main line, fifty miles of major, federal or state highways, and a large concentration of industries in populace area handling volatile materials. The enormous potential for wide-spread damage caused by natural or man-made disaster is obvious.

Plainfield is no stranger to emergencies. In 1967 we experienced a riot whose scars are still visible in terms of the social disruption and weakening of the community fabric, and subsequently have experienced floods, hurricanes, and power outages. Each of these emergencies was approached initially with the utilization of local resources. The need to effectively coordinate and communicate our strategies and activities became a very essential part of our activity. This requirement was needed not only for the purpose of addressing the immediate emergency but also the obvious need to enable local government to continue to function. During World War II and the subsequent years, we did maintain a "civil defense" capacity which was maintained at minimal levels and, frankly, served as a sort of a outlet activity for many of the persons who are associated with it. This is not to demean the sincerity of the government regarding this activity but the absence of any critical incidents during that time tended to cause apathy to set in which resulted in a reduction or obsolescence in the resources which were assigned to that function. I would like to move quickly to our experience during the 1967 riot. At that time, the emergency communications network consisted of a radio dispatcher for our police department and a radio dispatcher for our fire department. Each operated on a separate frequency and this was adequate for the conditions that prevailed during the very early phases of the disturbance. Shortly after we became fully aware of the magnitude of the

problem with which we were confronted. We, per procedures, notified our County emergency network which in turn notified the State authorities of the developing situation. Each of these communiques required the use of landline telephones and upon the arrival of the authorities from each of the jurisdictions, there was no overall methodology for issuing instructions or coordinating the responding units. As usually happens, we muddled through the emergency and based on our experiences and knowledge at that time, it should be concluded that the incident was handled quite well. However as a result of that experience, we identified some shortcomings and immediately took initiatives to improve our communication capability. We established an emergency operating center with input from State and County officials in coordination with an Emergency Management Committee which was made up of local public safety officials i.e. police and fire department, public works, health and welfare, engineering, national guard, hospital, rescue and City Administration. Each "expert" developed an Emergency Operational Plan for his activity that has been field tested and made a part of our overall Operation Manual. Presently, in the event of an emergency, the Emergency Council is convened and each member reports to the Emergency Operating Center (EOC) for the purpose of coordinating his activities. At this time, we are able to identify three separate frequencies for local operations. We assign one each to the Police Division and Fire Division, and the Department of Public Works. Each supervisor in those units can then communicate directly with his/her personnel plus have the ability to coordinate their activities.

with the other major units that are present in the EOC. We have the capacity for the county, state police, and the military, to operate from this location by activating "jacks" already tuned to their frequency. Additionally we presently have the capacity to monitor and communicate directly with county authorities. From the stand point of this local emergency manager, this capacity seems adequate for the emergencies over which local jurisdiction will have control. Our experience during windstorms and floods have certified its effectiveness and adequacy.

Without going into a long exposition on the necessity of effective communications, I think it is appropriate to address the cos-benefit ratio insofar as the utilization of sophisticated equipment is concerned. As stated, from the standpoint of a local emergency director, dealing with those problems which he or she may reasonably expect to befall this community, the capacities which I have outlined above seems adequate and responsible. The local police, fire, rescue, and medical needs are being met with this arrangement. Each of the frequencies is monitored by a base and specific messages to specific disciplines can be relayed from the base. In my opinion a capacity at the local level or all units to transmit and receive from all disciplines is an extravagance which can not be justified. A cursory review of the instances when that capacity might have facilitated a response or lessened damage is not evident.

At the local level, specifically Plainfield, New Jersey, we are able to switch channels on each of the assigned frequencies and monitor local transmissions from other Divisions within the City government. Scanners have been placed in several of the Supervisory vehicles (Mobile Units) but local budgetary constraints presently prevent such installations in each unit of rolling stock. Of course, an option, were it available, would be to equip every vehicle with the scanner and to adjust each portable (hand unit, walkie-talkie) with the technical capacity to receive and transmit to any radio-equipped City unit.

In the past this community has been served well and has rendered a rapid and adequate response to emergencies. In the case of natural emergencies, there has been sufficient lead time for the larger jurisdiction--i.e. the state--to communicate with County and/or via teletype with local jurisdiction in order that they prepare and make ready for the possible consequences. The several floods and wind related storms that have occurred have not "caught us by surprise". A close monitoring of weather, rainfall, etc. has given us adequate time to prepare. Locally, and again, I speak for this Municipality, we have installed warning devices in outlying areas that give us an early reading of the rate of rainfall, we are constantly monitoring weather stations, and the time factor in the relay of information has not adversely affected the response.

Another incident which occurred quite recently was the

damage which a tank truck sustained when it slammed into an overpass causing some of the tank's contents (highly toxic) to spill onto the roadway and required an evacuation of residents within an identified radius pending the transfer of product.

The communication resources which were described in the earlier incidents enabled us to alert community, emergency resources--both local, county, and state--and resulted in a response that more than adequately contained the situation. The on-sight operators--first responders--were in communication with their units and the matter, fortunately, ended without incident.

In my opinion one should look at the effect of traditional and advanced technology for local utilization in the context of the greater possibility for advanced technology on a wider geographic scale. I would now like to (refer to the Union County Emergency Communications System). Operationally, in Union County, each municipality will notify the County Emergency Manager whenever a situation develops which may be beyond the capacity of local resource to control. This direct and continuing communication with the County alerts additional jurisdictions of developments and allows the County to marshal and dispatch needed resources. Needless to say, disasters are often widespread and do not respect geographical boundaries. Thus, several communities are usually similarly affected and require County assistance. From the stand-point of the local Emergency Manager, a heavy dependence is placed on the resourcefulness and capability of the

county--both from a materials supply focus but also as a coordinator and evaluation of information.

1. Summary of Program, Projects Accomplishments

A. Problem:

In the 1960's Union County had one of the highest population densities in the nation with 543,000 persons in 102 square miles; 21 communities; two airports (one a major commercial); over 121 miles of railroad mainline; 50 miles of major federal or state highways; and a large concentration of industries in populous areas handling volatile material.

The lack of radio communication between Municipal Emergency Forces and an Emergency Operations Center at the county level was an obvious shortcoming requiring action. Three major air creases, a refinery explosion and fire, three Presidential Disaster Declarations for flash flooding, and a paralytic blizzard within the county emphasized this need over the years.

The Union County Board of Chosen Freeholders and the County Manager were supportive of the Emergency Preparedness Programs of the Municipalities, plus they sensed an opportunity to (1) gather intelligence on emergency situations, (2) coordinate the required assistance of emergency forces to minimize the loss of life and property, (3) improve law enforcement and traffic control in such periods and, (4) effect economies in

the normal operations of the county.

B. Solution:

The solution to these problems was initially begun by the Board of Freeholders in 1967, when it funded a CRIME ALERT 2-WAY RADIO SYSTEM (commonly referred to as the HOTLINE). Using a new frequency, all 21 municipal police departments were tied in with the Sheriff's Office, the Prosecutor's Office, and a State Police Barracks (no longer in operation). As a result, the Prosecutor's and Sheriff's mobile operations were expanded to include the State Police frequency. This supplemented the existing county radio systems of the Park Police, Park Maintenance and Road Departments which consisted of three frequencies, three base stations, and approximately 40 vehicles. During power outages, no other county departments had communications and no emergency power units were available, except for the HOTLINE.

C. Achievement:

To meet what it considered its obligations, Union County has constructed in a most economical manner, a Communications System that can quickly cope with threats to life or property.

Union County has effectively tied together 21 municipalities' Police, Fire and Rescue units and seven Private Emergency Hospitals' Communications Systems for varied emergency responses. Such operations can be coordinated from a single Command Post or Mobile Command post.

Emergency power generators are now situated at the Courthouse, New Administration Building, Jail, Juvenile Detention Center, Road Department, County Police Headquarters, Communications Division, Emergency Operating Center, and the County Hospital.

A radio system has been developed that includes:

24 Base Stations using 12 frequencies, 126 cars, 7 vans, 69 trucks, 117 portables, and 110 pagers.

II. Background of Program/Project

A. Role of County:

The following describes the county's role of filling gaps in critical emergency communication areas:

- 1970 An Emergency Operations Center was constructed for the county's Civil Defense and Disaster Control Division, equipped with Radio Amateur Civil Emergency Service Radios, then operated by ham radio operators.
 - 1973 A Radio Department was established and initially titled "Technical Services: consisting of a department head, a technician, and a clerk. They were to review and maintain the existing communications systems and plan the development of a coordinated communications system to meet the county's needs. Much later, they were given responsibility for the security and fire alarms, smoke detectors, and public address systems throughout the county's facilities. Two more technicians were added after one year.
 - 1974 Communications Division (formerly Technical Services) purchased a 4-wheel drive vehicle to serve as a service truck, and eventually as a Mobile Communications van.
- At the recommendation of the County Civil Defense and Disaster Control, the county purchased and installed 13 ambulance/hospital radios in ambulances in those communities unable to acquire them from federal funding sources.

The Prosecutor's Office successfully obtained a federal grant to provide ten portable radios for use by the county's Tactical Police Force, a unit composed of 100 volunteer police officers from all municipal departments.

The Communications Division established radio systems for the Mosquito Control, Shade Tree, Bridge, and Engineering Departments with a few new radios and conversion of radios formerly used by the Prosecutor's Office.

- 1975 Replaced 29 Base Stations for Police Hotline Radio System in all law enforcement headquarters, and refurbished repeaters.

Developed backup repeater systems at other secure locations.

- 1976 Equipped County Emergency Operating Center with refurbished Police Hotline and Public Works base radio stations, and new base stations on County Fire Radio Net and N.J. Hospital Emergency Administration Radio Net (HEAR).

Civil Defense purchased hospital/ambulance radio for Communication Division's Mobile Communications vehicle.

- 1977 The Communications Division initiated radio-maintenance contracts with five towns, effecting economies for them.

County Civil Defense purchased three base stations on the County Fire frequency. These were installed in communities not operating on that frequency which completed the link to all 21 fire departments, though many municipalities have local frequencies for local operations.

County Civil Defense installed an Administrative Telephone for County Fire Mutual Aid. (Linden Fire Headquarters donates the services of its dispatchers to direct that program and pays all expenses.)

Newark International Airport Control Tower has a direct wire link to Newark Police Headquarters, who has a County Hotline Radio to alert all of Union County if an aircraft is in trouble.

- 1978 The county initiated a program of obtaining portable radios on the Public Works frequency for numerous county officials who may be needed in an emergency or who may be contacted by the County Manager at various times. Twelve were purchased initially and more added

later.

Through the use of jacks from other departments, six additional telephones (with none-emergency responsibilities) were added to the Emergency Operations Center with minimal expense of 50¢ a month each. This expands the total to 13, including special units for the County Manager, Police, Fire, Rescue, and Public Works Departments.

Major construction change in the Emergency Operations Center provides a Command Room for the County Manager and key officials which is separate and apart from Communications and Operations areas, but with continuing visual supervision.

County Civil Defense purchased two new 50-channel multiband scanners which were installed in County Police Headquarters and County Fire Mutual Aid Headquarters.

1979

All County Repeaters were replaced, along with antennas.

A new building was constructed at the Mountain Repeater location which houses the radio apparatus and emergency generator unit. This action was dictated by weather damage and juvenile vandalism.

To assure availability of all essential officials on an individual or recall bases, the county purchased 110 pagers operated by the County Police which, in addition to alert tone, can provide a 15-second message. Included in this group are the County C.D.D.C., Volunteer Staff Officers, the County Fire Coordinator, the County First Aid Mobilization Coordinator, and County Radef Coordinator.

The County Police Department (formerly the Park Police) has been established as the monitoring and dispatching center for all county public safety communications. The Communications Division has developed a cross-patch system for county radios through which key county officials may talk directly to other systems under the control of the County Police during serious emergency situations.

B. Means of Financing:

The bulk of funding has been borne by the county, with the exception of some grant-in-aid funding for C.D. radios and a generator, and L.E.A.A. funds for Tactical Police Radios.

C. Legal Requirements:

The county's only legal requirement is under the State's Civil Defense and Disaster Control Act of 1953, which requires that an Emergency Operations Center must be constructed and equipped with appropriate communications. Union County has gone well beyond that with sound planning and economical programs to meet both its own needs and those of the communities it serves.

III. Future Programs

The Civil Defense and Disaster Control Division is seeking to purchase or refurbish a radio for County Fire Mutual Aid on a State Fire Command frequency, which will tie it into the Fire Mutual Aid headquarters of other 20 counties in the state, and is awaiting installation of a Federal NAWAS phone connecting County Police, State Police, and weather officials.

If a proposal currently under study is approved, the County Communications Division will expand its present staff to more effectively serve the Communication Maintenance Program needs of the county's communities.

Another proposal is under consideration to radio-equip, under a new frequency, all vehicles used by county or

social services to transport elderly or handicapped persons. This would expedite information on traffic conditions or summon aid quickly if the situation required such action.

In the State of New Jersey there is an almost natural "chain of command" regarding emergencies as they develop any place within the State. This "chain" is from the local to the County to the State authorities. At the local municipality level it is not uncommon to consider that unit as working very very closely with the county activity. Local resources are limited and it often becomes necessary, through mutual aid pacts, to reach beyond a local boarder to utilize the resources of another community. A map will indicate that Plainfield is in the northwest corner of Union County and it is significant to note that we boarder two other counties from which we can often gain quicker access to materials than we would were we to rely on the County seat--some fifteen miles away. Through custom, it has been our practice to reach into neighboring towns--in neighboring counties--for a quicker response to local emergencies. This mutual aid pact, although it crosses county lines, has been recognized as a responsible manner in which to respond to emergencies. In Plainfield, we still have the direct "chain" to our County facilities and when their resources are made available we are then able to release our neighboring counties resources. This has proved a most effective way of dealing with the emergencies in this particular quadrant of the County.

I have attempted to present the prospectives from a local emergency manager's point of view and the opinions expressed herein are my own. I have had conversations with persons who have some responsibility both locally and on a wider jurisdiction who feel that more sophisticated equipment which is presently being marketed would enhance the overall capability for effective communication. It is hoped that this Committee will receive a presentation from the proponents of the "State-Wide Plan".

May I conclude by stating that the essence of management be it organizational or emergency--is communications. Presently, there is room for improvement at the local level. Technology is enhanced almost daily and I feel that with minimum expenditures a "more perfect" system can be developed which would meet needs of the service. It would be my personal hope that we reduce the incidents of crime and the fear levels of crime and thereby make a greater contribution to the stability of our society rather than to engage in a expensive, costly, rapidly changing, technology in the area of emergency communication which is considerably beyond what I feel the actual needs to be.

The options available in the area of communications technology are vast and the weighty problem of identifying "the best" option during a changing technology only further argues on behalf of delay. However, there are some real needs which cry out for early resolution and I urge the Committee to give this matter of providing safety--regardless of the nature of the threat--to the citizens of this Country as a primary responsibility of Government.

Mr. GORE. Thank you very much, Mr. Allen. I might add for the record that in addition to your responsibilities in the State of New Jersey, because of your excellent record, you serve on the National Academy of Sciences' nine-member board in this area, and you bring that expertise and distinction to this subcommittee hearing as well.

If you could redo your system, starting from scratch, with no limitations imposed by the past development of your system, what would you do differently? How would you set it up?

Mr. ALLEN. I would move offsite—that is, I would move out of the heart of my municipality some 4 or 5 miles' distance. I think that has psychological as well as operational advantages.

During an emergency, those persons directly involved in the planning and control of this emergency must be away from the distracting influences that generally occur in our emergency operating center. Our economics dictated that we place it where it presently is.

I would go for a single radio band in terms of my police, fire, and public works people. Of course, when we get to the county, State levels, or the military, they have their own, but for the local operation during an emergency, I would have them on a single frequency so they could communicate directly with each other without the necessity of going through base or even interrupting transmissions of a particular nature.

As I indicated earlier in my particular position it is somewhat unique in that I can control administratively and operationally the first responders to any emergency. So, by getting on my band, I am in direct contact with the supervisors of each of those three operations. My colleagues in this operation don't have that same advantage, but I would reduce the number of transmissions; I would reduce probably the number of transmitters, because it has been my experience that so often when an emergency develops, we are just inundated with transmissions under the guise of information.

We do need information, but we must cut down on transmissions. As a local operator, a little country boy, if you will, in this whole scheme of things, if the technology cannot be used by me and dozens of other persons with whom I work, it is going to be of little value. Many of us are appointed, so every 2 or 3 years the membership on our committee changes, and if we are not getting people thoroughly familiar with the utilization of this technology, it is going to be more harmful than helpful. I would keep my communications simple; I would not want them any more sophisticated than the need dictates, and I would attempt to reasonably and responsibly determine my needs based on the experiences that we have had to date.

Mr. GORE. An interesting, helpful response.

Can you describe briefly the mutual-aid arrangements between your city and nearby localities?

Mr. ALLEN. I live in an urban center. As such, most of our public emergency forces are paid employees. We have a paid police department who resemble the hole in a doughnut. Many of our neighbors are volunteers. They are not as industrialized as we are.

Whenever a situation arises which taxes the capability of that local entity to respond, we then engage in what we call a mutual

aid assistance pact by notifying a central base, indicating what are your needs. Resources from neighboring municipalities are deployed to your facility or your area, placed under your general command to assist in controlling that conflagration.

Plainfield is situated in the northwest quadrant of Union County. Technically, by chain of command, we should have mutual aid with county resources. However, due to our unique location we rely on the resources of two neighboring counties who are closer to us than the next larger city in our county. This works out well. The agreements have been reduced to writing. The liabilities have been established, and it works extremely well.

No one in our particular area seems to have an advantage. We as an urban center have occasion to call upon a neighbor. They often have occasion to call on us. We have the greater amount of manpower; we have more sophisticated mechanical equipment, but the utilization of the mutual aid pact has never been a cause of disruption or disagreement among the participating agencies.

Mr. GORE. That is very interesting.

Have you in your community participated in regional simulated emergencies or tests which required so-called vertical communication involving the local State and Federal decisionmakers?

Mr. ALLEN. Yes, we do. As I indicated, we have an airport, Newark International Airport some 30 miles from us, and as part of their training, they simulate incidents quite frequently. We participate in that. At one time, I was in charge of the emergency forces at Newark International Airport.

The county conducts exercises two to three times a year, and all 21 municipalities are expected to participate in the county exercise. At the local level, we conduct one to two exercises per year. The scenario is in conjunction with the county and State authorities. They encourage other municipalities to witness the operation, and here again, I think one of the good things that we have in New Jersey is that, as far as I can determine, the petty jealousies that may exist in other agencies seem to be at a minimum in New Jersey.

Most of the local managers invite criticism of their operation. Through our State organization and our county organizations we meet frequently, we critique each other in a spirit of good will, because any such incident could happen in our community. Our organizations are not only social, but they do serve a professional purpose, and exercises in New Jersey are not uncommon.

Mr. GORE. Very good. I have the feeling we could learn a great deal more from you in a more extended dialog, but because of time pressures, we are going to have to move on.

I would like to again thank you for an excellent presentation and contribution you have made to our proceedings.

Your perspective is invaluable. Thank you so much for appearing here today.

Our next witness is George M. Hicken, project manager with COINS at the National Security Agency. Mr. Hicken, we are delighted to have you here. We look forward to your presentation.

STATEMENT OF GEORGE M. HICKEN, PROJECT MANAGER,
COINS, NATIONAL SECURITY AGENCY

Mr. HICKEN. Thank you, Mr. Chairman. It is a pleasure to be here today.

What I hope to do in the next few minutes is to share with you some of our experiences in building two networks where we have netted information computers in different agencies together to serve operational needs of many agencies. I will try to cover this in four different areas, beginning initially with a little bit on the history of how we got started, a little bit on the current network, some of the things we are doing with current technology that might be useful to you, and, last, a little bit about our management structure.

In the early part of the 1960's, the National Security Agency was building its first remote information storage and retrieval system, known as the TIPS pilot system—the technical information processing system. The goal of the system was to determine whether or not file sponsors could update their files on line within the building and also to retrieve—while other users in the building could retrieve information as they needed it, in a timely fashion.

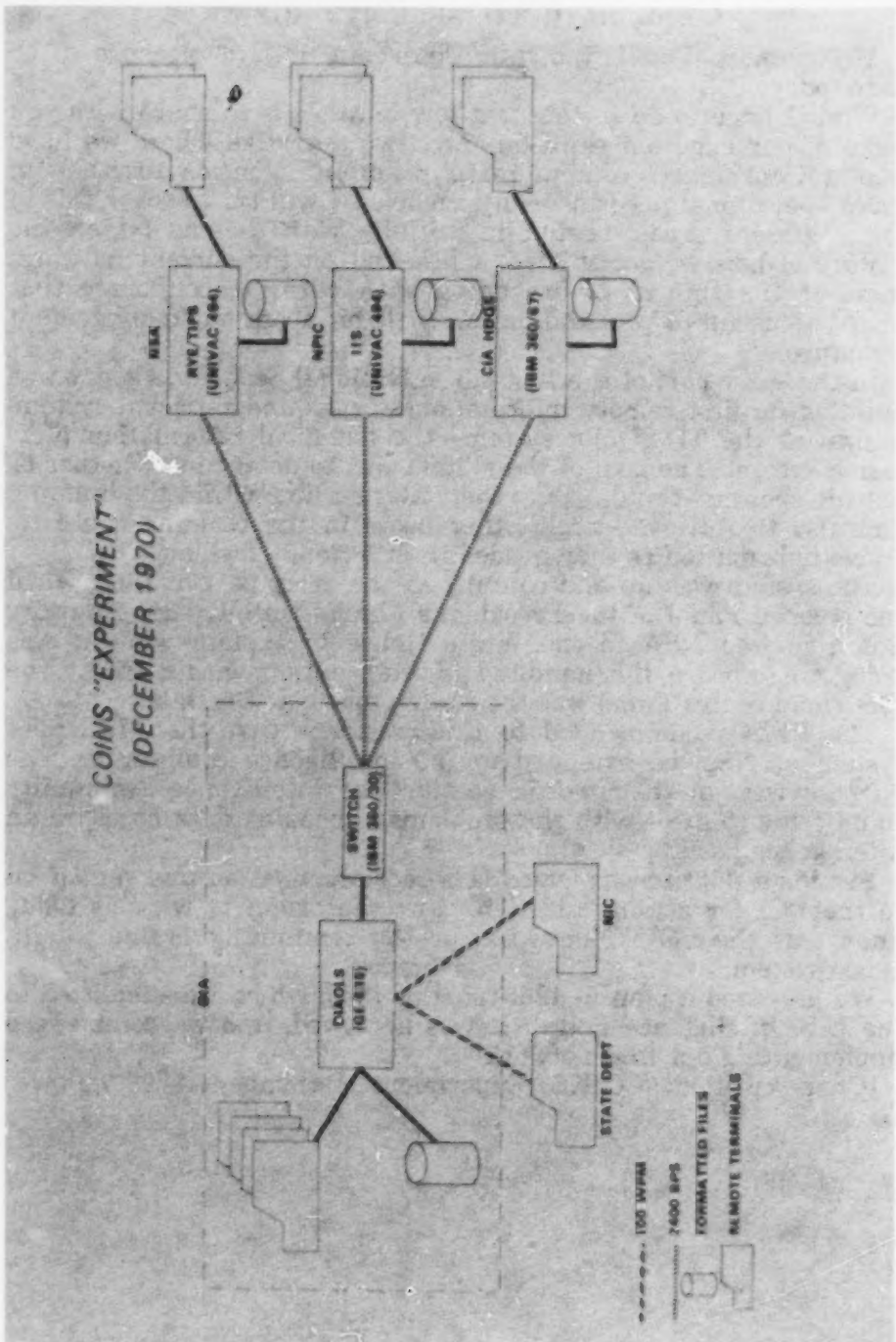
The system was up and running in the early part of 1965, when the Science Panel of the President's Foreign Intelligence Advisory Board invited NSA to the White House to explain what it was doing to improve the handling of information within NSA. The Chairman of this Panel was the leadoff speaker, Dr. Baker.

The PFIB recommended to the President that the TIPS pilot system at NSA be extended to the intelligence community. The purpose was, in their words, so that the intelligence community could come to grips with the problems of sharing data bases on an interagency basis.

President Johnson endorsed this recommendation and sent it on to the DCI for action, and it became the origin of what is today known as the COINS network, or the community online intelligence system.

We prepared a plan in 1965, part of 1966, which we submitted to the U.S. Intelligence Board. It was approved, and we commenced implementing our first network.

[Chart entitled "COINS 'Experiment' December 1970" follows:]



Mr. HICKEN. What I would like to say while they are getting the projector and slides ready is that we took a number of existing information storage and retrieval systems in the intelligence community which were already in place, already servicing the needs of these various agencies and linked them together, so that users could share information online between agencies and between organizations. That was the main charge.

The problems that we encountered in doing this, were that all these systems were already in place, already servicing an agency. We also encountered other problems such as, each system had its own information storage and retrieval language for retrieving data, and they were different. Most of the retrieval languages were homegrown, tailored for the agency's needs in which they were located.

The slide before you entitled "COINS 'Experiment'—December 1970," is the network as it looked in 1970. As you can see, there are four host file processors in the network, one at DIA, one at NSA, one at NPIC, and one at CIA headquarters.

The users sitting remote terminals in these agencies could not only access their own data bases, but could access the data bases in any one of the participating agencies, online.

The one characteristic that all of the host file processors had, at that time, was the fact that they were all batch retrieval systems. You put a query in; it went through the network; and 15 or 20 minutes later you would get an answer back. They were not interactive systems in the true sense of the word today.

The State Department and the National Indication Center, had remote terminals off the DIAOLS system at DIA, so they could also have access to the data bases, although they did not have a host processor of their own with their own remote terminals.

The computers were all interconnected, using 2,400 baud, voice-grade circuits.

This is the network that we first established and, as I said, we had about 30 data bases that were available on different systems that users could log on and use. We had the multiretrieval language problem. We had the multiple data standards problem; everybody had different ways of recording the same information. And this presented us with a unique problem of how do you train the users in these different agencies to use all of the retrieval languages and use the assets available in each of the systems.

It also presents a management problem on how do you manage these diverse resources and bring them together so they can all interoperate and intercommunicate together.

The network survived, and it operated. When we first started out with the proposal it was predicted that it could not be done because of all the diverse hardware that was to be interconnected; different kinds of remote terminals and different computer systems. Well, we did it. Then the prediction was, nobody would ever use it. As it turned out agencies did use it when it was made available, even though it was not convenient because of the multiple retrieval languages and lack of data standards. However the users did find a way to make it work and began to use it operationally.

[Chart entitled "Purposes of COINS" follows:]

PURPOSES OF COINS

- INTER-AGENCY SHARING OF
DATA BASES
- REDUCES INTER-AGENCY FLOW
OF REPORTS
- REDUCES NEED FOR MULTIPLE
TERMINALS
- PROVIDES USER SERVICES OF
COMMON CONCERN

JULY 78

UNCLASSIFIED

Mr. HICKEN. The purposes of COINS are very simple. The first thing it has done is to permit the intelligence community to take advantage of the economics of sharing data bases on an inter-agency basis. This is a major goal of the COINS program.

Another purpose is to reduce the interagency flow of reports, both in electrical and hard copy form, and some agencies have actually stopped producing hard copy reports and electric reports, and now users retrieve the information online. They don't have to have the data sent to them electrically. They don't have to have it in one sort, printed and listed. They can retrieve it in a number of different formats when they need it.

It also reduces the needs for multiple terminals you have a single terminal in your agency on your system, and you can access any other system in the network to which you are authorized access. You eliminate what we term in the business terminal illness, where you have a separate terminal for every system in the network that you want to access. In some rooms you have gone into, I know, you will have a whole fleet of terminals, a separate terminal for each system being accessed. In addition the COINS network also provides some user services of common concern which are across the network, such as electronic mail service, text editor and other user aids.

[Chart entitled "COINS Users Advantages" follows:]

COINS USERS ADVANTAGES

- **SELECTIVITY**
- **FLEXIBILITY**
- **TIMELINESS**
- **CONVENIENCE**

Mr. HICKEN. Users like COINS because they have the selectivity. They can select only what they want to see at a moment in time out of the data base. And they have the flexibility of having the information retrieved formatted to suit their needs. Although you and I may both select the same information for retrieval, we can each have it formatted and displayed in a different way to serve our unique needs. COINS service is much more timely and much more convenient for users because the information is being displayed on remote terminals located in their operating area.

[Chart entitled "ARPANET Geographic Map, July 1981" follows:]

ARPANET GEOGRAPHIC MAP, JULY 1981

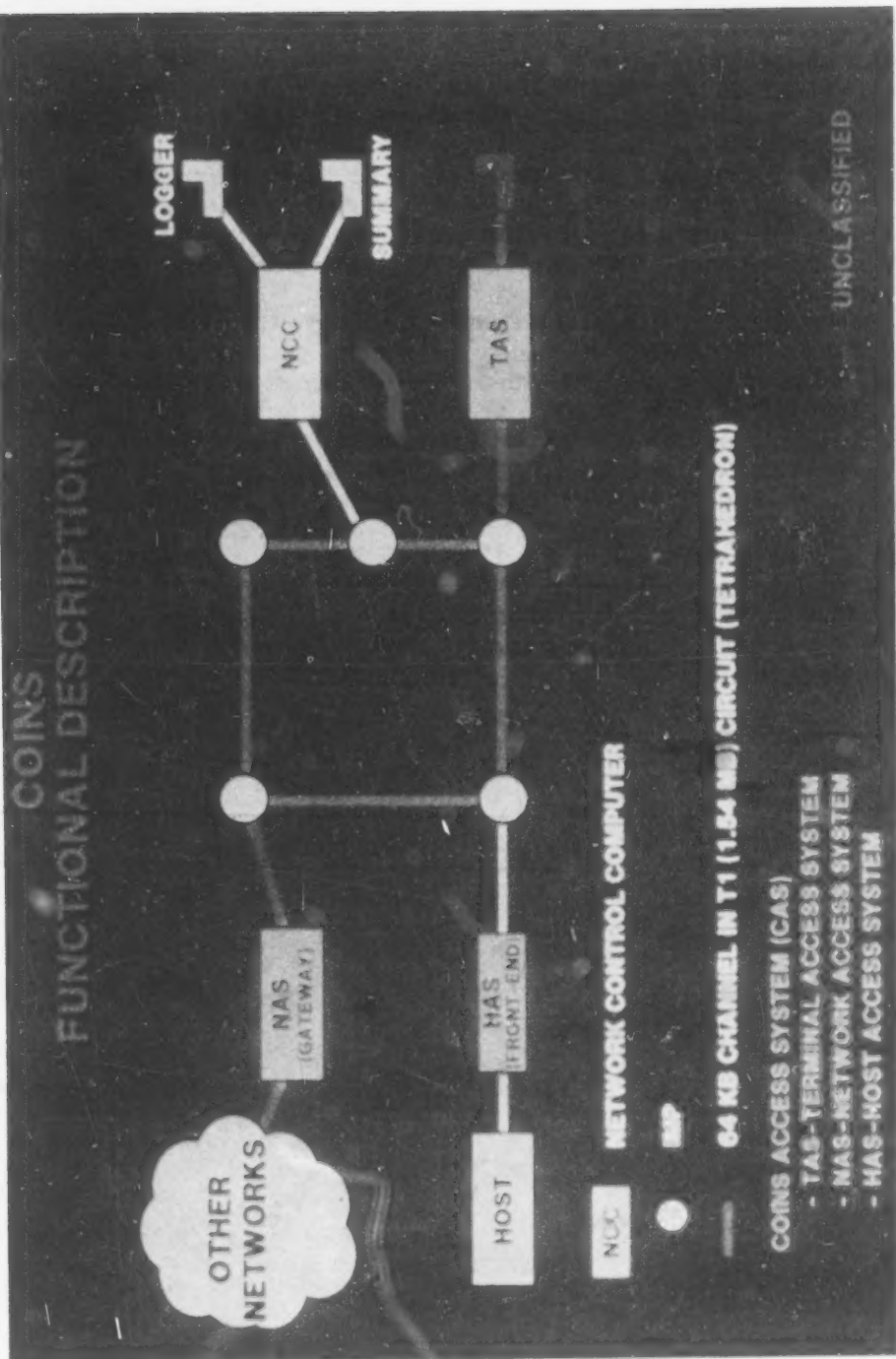
Mr. HICKEN. In November 1972, the DCI decided that it would be an opportune time to have the COINS "experiment" evaluated, and he appointed a high-level committee chaired by the Deputy Assistant Secretary of Defense for Intelligence. They commenced a 3-month evaluation of the COINS experimental network that you see on the board.

They submitted their report and recommendations to the DCI. They concluded that the intelligence community needed to build a more robust network; a network that not only handled batch and interactive queries, but also a network that had alternate routes of communication.

We made a study of the networks that were then available in the country. The ARPANET, which was up and running was one of the networks examined. We decided that the fastest way to build a new COINS network was to transfer existing technology, and not go out and invent our own communications processors and protocols.

We chose to use the ARPANET. We built a mini-ARPANET on which we built our second network, or what is known today as the COINS-II network. We just transferred ARPANET technology lock, stock and barrel over to the COINS II network. Now, this is a current diagram of the ARPANET. But I think it is important because we will talk more about it later on, particularly the satellite circuit on out to Honolulu.

[Chart entitled "COINS Functional Description" follows:]



Mr. HICKEN. This is a functional description of the COINS network. The dots there are the interface message processors, the ARPANET IMP's. We are using the Honeywell 316 IMP's in the COINS network and they are interconnected, using a 64 kb channel within a T-1 carrier. This is a direct transfer of ARPANET technology. In fact, usually we run one release behind the regular ARPANET on IMP software. They test it first in ARPANET, and once all of the kinks are worked out of it, we transfer the software over to the COINS network and deploy it operationally.

We also have a copy of the Network Control Computer that is used on ARPANET, which monitors the network in near real time and gives the controllers in the COINS Network Control Center [CNCC] the capability to monitor the network. Each IMP reports back to the Network Control Computer every 52 seconds on the status of its communications circuits, the status of its own operations and the status of the host processors connected to it. We now have a capability of monitoring the network.

We have built gateways to other networks. The COINS network is interconnected to two different networks. One is a resource-sharing network which has files and host processors, which COINS users can access. The other network we are using a backbone network which we are using just to communicate traffic. We will talk more about both of these interconnections later.

In connecting a host processor to the network we have chosen a Host Access System or front-end processor, this approach minimizes the amount of work that has to be undertaken by the agency in which the host file processor is located. The agency has to write a little software to interface its host file processor to the Host Access System. The amount of work as I say, is trivial. We have the protocols worked out to interface but they have to be tailored for the particular manufacturer's line of hardware and software we will be interfacing as a host file processor.

Then, on the other side, we installed a Terminal Access System [TAS]. When we first started out, we thought we would only have on TAS with six or seven remote terminals. The Terminal Access System is designed to provide remote terminal service to those agencies and organizations that need access to the network, but which do not have a host processor and terminals of their own or can't acquire them on some other agency's system in the network.

As I say, we initially thought we would have one Terminal Access System and perhaps six or seven terminals. We now have 54 terminals on three Terminal Access Systems, and in addition we have 4 more TAS's being installed. The IMP-software, I might point out, if you are familiar with ARPANET, is controlled from the CNCC. You can down-stream-load the software to any IMP in the network; you can run diagnostics on any IMP from the CNCC.

Similarly, with the Terminal Access System, the system software in all of the COINS Access Systems are controlled from a single point—the master TAS in the CNCC. We downstream load the software for the CAS's through the network. We control the software in all CAS's through the network and update it through the network. That gives the COINS PMO total control over the environment in which it is responsible for operating and managing.

[Chart entitled "TAS Capabilities" follows:]

TAS CAPABILITIES

- SINGLE LOG-ON PROCEDURE
- SECURITY
- QUERY STORAGE
- ANSWER STORAGE
- TEXT EDITING
- ELECTRONIC MAIL SERVICES (EMS)
- MULTI-RETRIEVAL LANGUAGE TRANSLATOR (ADAPT)
- CREATE USER FILES (PUBLIC AND PRIVATE)
- MAN MACHINE RELATIONSHIP SOFTWARE
- TIME-TRIGGERED QUERIES (FUTURE)
- TELECONFERENCING (FUTURE)

UNCLASSIFIED

Mr. HICKEN. Now, the Terminal Access System has some interesting capabilities, which are the same for all of the COINS Access Systems. The goal, as I indicated earlier, was to provide users with a single terminal by which he could access any of the systems in the network to which he was authorized access. But we also wanted to provide the user with a single log-on procedure, and a single security procedure whereby he had to learn only one password. He doesn't have to learn a separate password and a separate log-on procedure for each system in the network to which he is authorized to access.

You will see in some instances today, users carrying around a little notebook to see how they log-on to a given system and what are their passwords user identification for each system. The goal is to establish this single log-on procedure and we have been very successful.

In addition the users have the capability to store their favorite query. If they have a query they ask all the time, they can store it, call it up, change the values, and enter it in the network. They can temporarily store their answers.

We have text editors available on the CAS's, which permits a user to write reports in upper and lower case. We have a Electronic Mail Service, which permits a user to send these reports around and ask his colleagues in the network to comment on them.

Another major problem which I talked about a little earlier was the multiretrieval language problem. A few years back, ARPA funded a major program for the COINS PMO aimed at developing a multiretrieval language translator that would actually let a user use one retrieval language to go to four separate retrieval languages in the network.

The prototype system was developed, installed, and then we asked Mitre to come in as an independent group and make an evaluation of the prototype system. Based on their evaluation we are now in the process of building our first operational translator which will be delivered this month or next month. The translator will be, again, evaluated initially by Mitre, and then if their evaluation looks good, we will turn it on for a few users to begin to use. Later, Mitre will come back, after users have had an opportunity to use the translator for 6 to 9 months to determine what the users' reactions are to this capability. But the goal is to give the users one language to access any system in the network. Just like we are giving them one terminal to access any system in the network.

The alternative to using a multiretrieval language translator is to go to every agency and say, "We are going to buy you common hardware; we are going to buy you common software and a data base management system." It is very expensive and a very difficult thing to sell.

Users can also create their own public and private files, public in the sense that they share them with other users on the network, or private files are those that they keep for their own use.

Another large program that is being funded by ARPA is the man-machine-relationship program [MMRP]. Software and hardware from this program are available and it includes some new types of terminals. Objective of the program is to try and improve the interface of the user to the network.

For the future we have time-triggered queries, and these are queries which you might like to ask every morning when you come to work. Instead of actually sitting down and putting them in, you can set the queries up and they will run automatically for you just before you come to work, so then when you do come to work and log-on you will find the answers to your queries in your mail box. These are repetitive type queries that could occur every Monday morning, every Tuesday morning, first of every month, or whatever the case may be. It is a poor man's version of the Selective Dissemination of Information [SDI]. It is difficult to get each of the agencies to install and SDI capability with user profiles in their systems to answer such queries based. We go around and do it the other way, but it achieves the same effect.

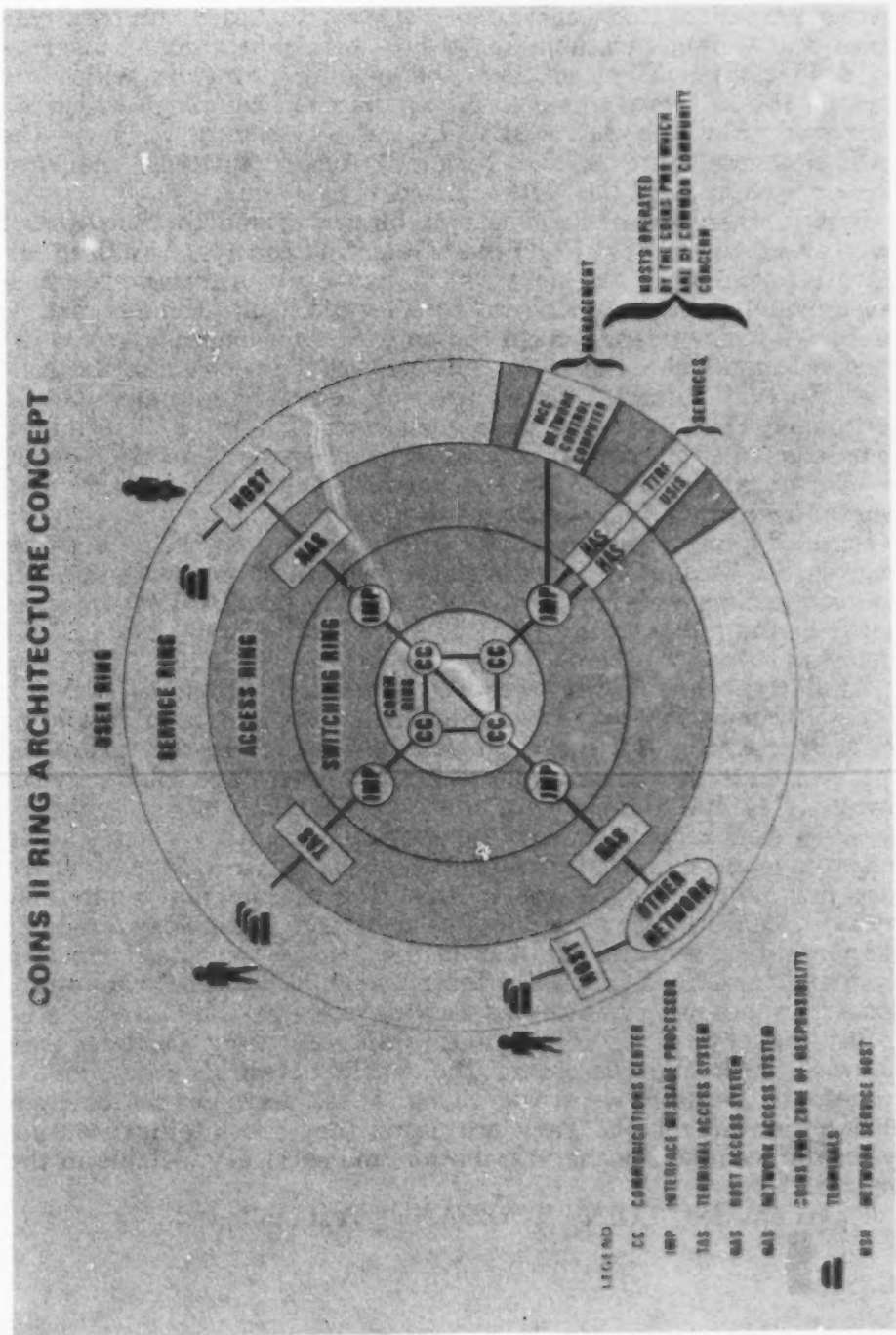
Mr. GORE. Did you say this is the poor man's version?

Mr. HICKEN. Yes. In this case you have to put the time-triggered queries in the CAS's as opposed to having your profile in the host processor triggered to send you the information you requested when it becomes available.

Teleconferencing is another feature we have looked at, and it is certainly in the future. It is asynchronous where you can log-on and maintain a conference with your colleagues in other parts of the network.

These are some of the kinds of capabilities that are available and some that we are considering, for the future.

[Chart entitled "COINS II Ring Architecture Concept" follows:]



Mr. HICKEN. Now, this is another way of viewing the COINS network, and in a conceptual sort of way. In the center ring you have your Communications Centers [CC] which are linked together by a T1 carrier. Then we have the switching rings in which are located the interface message processors the technology which we borrowed from the ARPANET. In the access ring we have the COINS access systems, the Terminal Access Systems, the Host Access Systems, and the Network Access Systems.

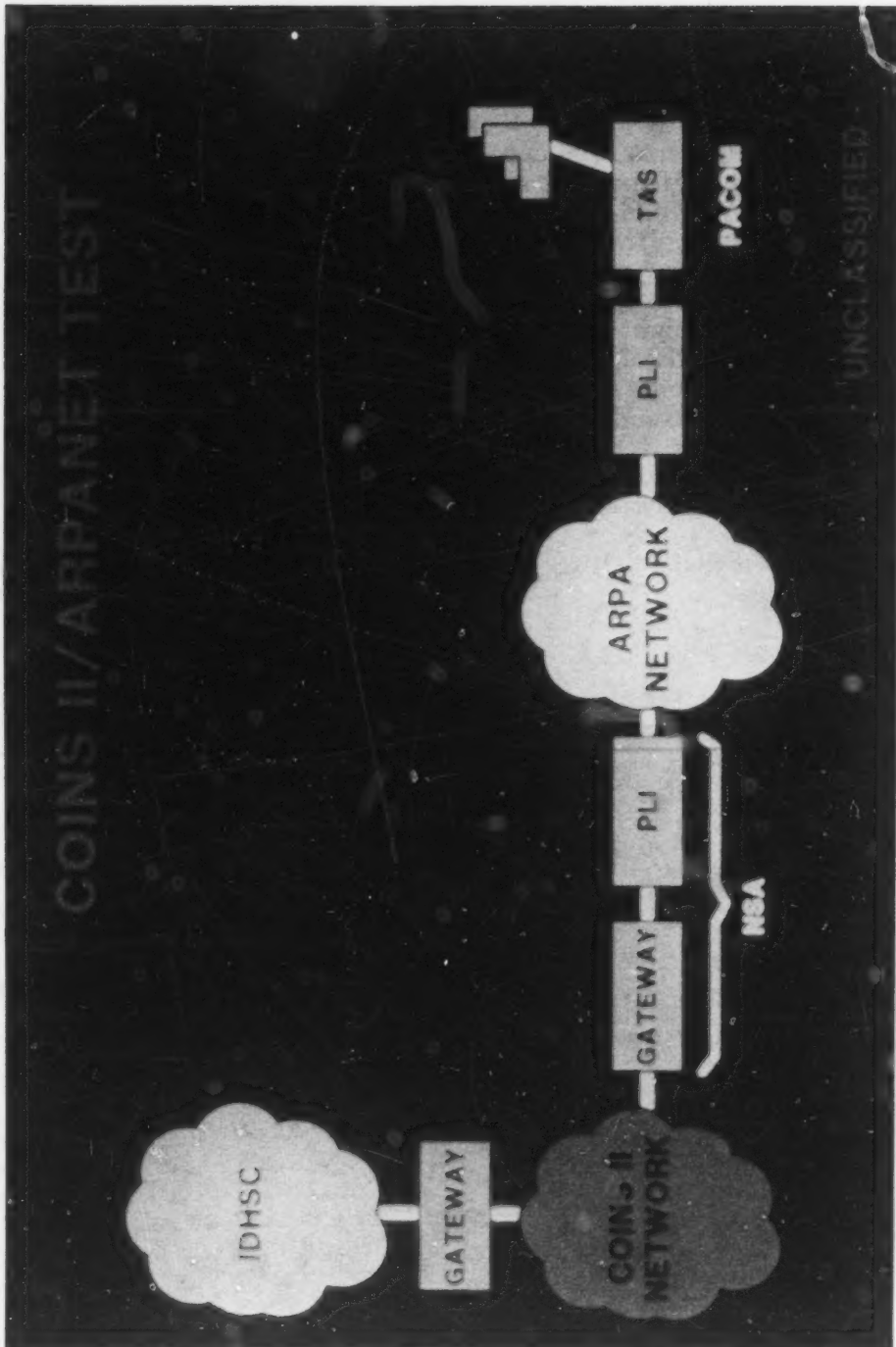
It is in these two rings, the switching ring and the access ring over which the COINS PMO has most of its control. Any user can have a terminal on the network, he can use the terminals which we provide, or he can bring his own terminal into the network. If he brings his own terminal in the network—for example, a Hewlett Packard or a Delta Data—we will convert it to look like the Network Virtual Terminal. So we are not tied to having any specific terminals. They just must be a modern-day CRT-type of terminal. If user is using a terminal connected to a Terminal Access System, he can go anywhere within the network or on out to other networks to which COINS is connected.

Similarly, any agency can add or connect a host to the network very easily. We provide most of the software and hardware to make the connection; we provide the protocols to bring a host into the network and make it very easy for agencies to add or delete a host from the network.

Similarly, other networks can be connected through a Network Access System, and they have their own hosts and terminals in it. We call that ring out there the service ring where the terminals, the host and other networks, are located. There are some services available in the service ring that the COINS PMO provides of common community concern. We provide computers which handle network management such as the Network Control Computer. We also provide host processors in this ring of common community concern. One is known as the TTRF, or the Technology Transfer Research Facility, and another is the User Support Information System. These are facilities in the network of common community concern, sponsored, maintained and managed by the COINS PMO.

But the outer ring is the most important ring in the entire network. It is the reason for the whole network's existence. It represents the users we are servicing. These users are not computer-oriented individuals. They are users; they are intelligence analysts who want to use the information and services available in the network.

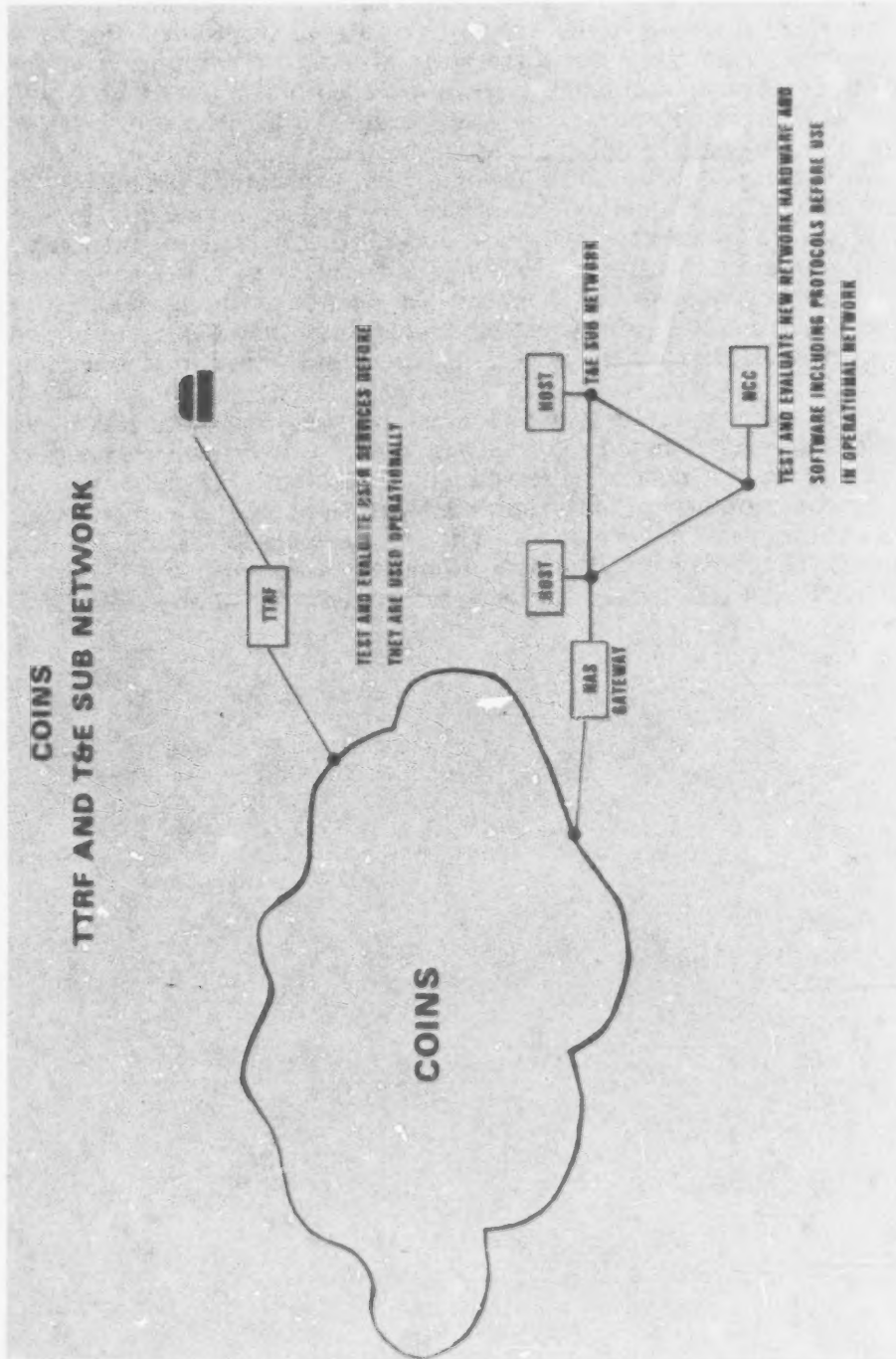
[Chart entitled "COINS II/ARPANET Test" follows:]



Mr. HICKEN. A few years ago, we were asked to determine whether or not we could actually make use of an unclassified network such as ARPANET. We constructed a gateway with PLI's on either side of it, and we installed a Terminal Access System in Honolulu. Analysts now sitting in Honolulu can interrogate data bases in the COINS network in either a batch or an interactive mode depending upon the capability of the host they are accessing, just as easily as if they are sitting at terminals in the Washington, D.C. area. They can go through another gateway into the DIA-managed network, the Intelligence Data Handling System, communications, which supports data, the unified and specified commands and military services, and access hosts in that network.

The PLI's, I might indicate, are devices which have been developed for use in the ARPANET. They are called private line interfaces, By which data is encrypted before it goes out on ARPANET and in addition it adds a network header in the clear for transiting through the ARPANET. When it arrives PACOM, the clear header is stripped off and the text is decrypted and sent on into the Terminal Access System. The data is fully protected in an unclassified network.

[Chart entitled "COINS TTRF and T. & E. Sub Network" follows:]



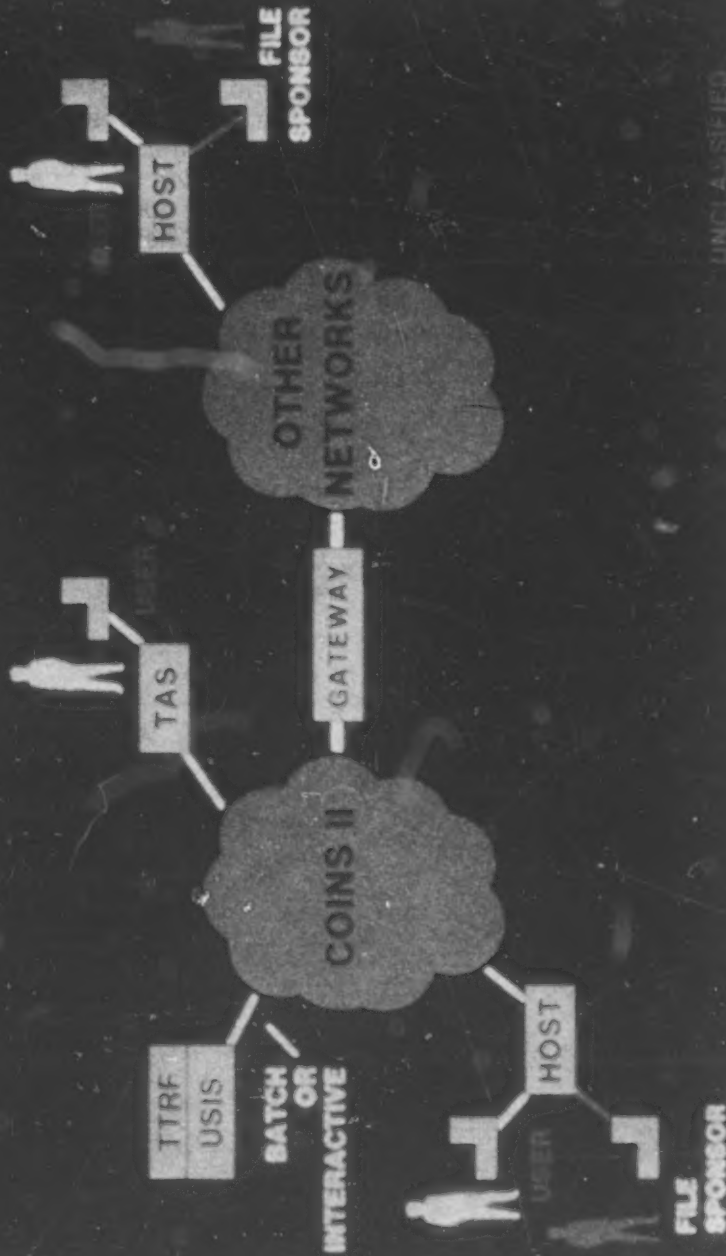
Mr. HICKEN. As I indicated earlier, we have two different kinds of test facilities. One is the TTRF, where we test new user software. Here is where we will be testing the multi-retrieval language translator. This is where Mitre will be doing its evaluation of the multiple-retrieval language translator. Also being tested here will be the User Support Information System (USIS), the pilot system which is now being implemented.

We are also testing some other software provided by ARPA, as part of the man machine relationship program. The TTRF is a place where we can test software and hardware without interrupting the operational users. However, if we want to make some new software available to the users on the network, we can do it very easily in order to obtain their reaction. These new tools, are aimed at improving the interface of these users to the network and their use of the network.

We are also installing a test network. The test network is designed to test out new protocols, and new hardware which we may be using in the network. We can hold tests in this network and operate a number of different configurations without disrupting the main operational network. When these tools look good, we can transfer them over into the operational environment.

[Chart entitled "Users Support Information System—USIS" follows:]

USERS SUPPORT INFORMATION SYSTEM (USIS)

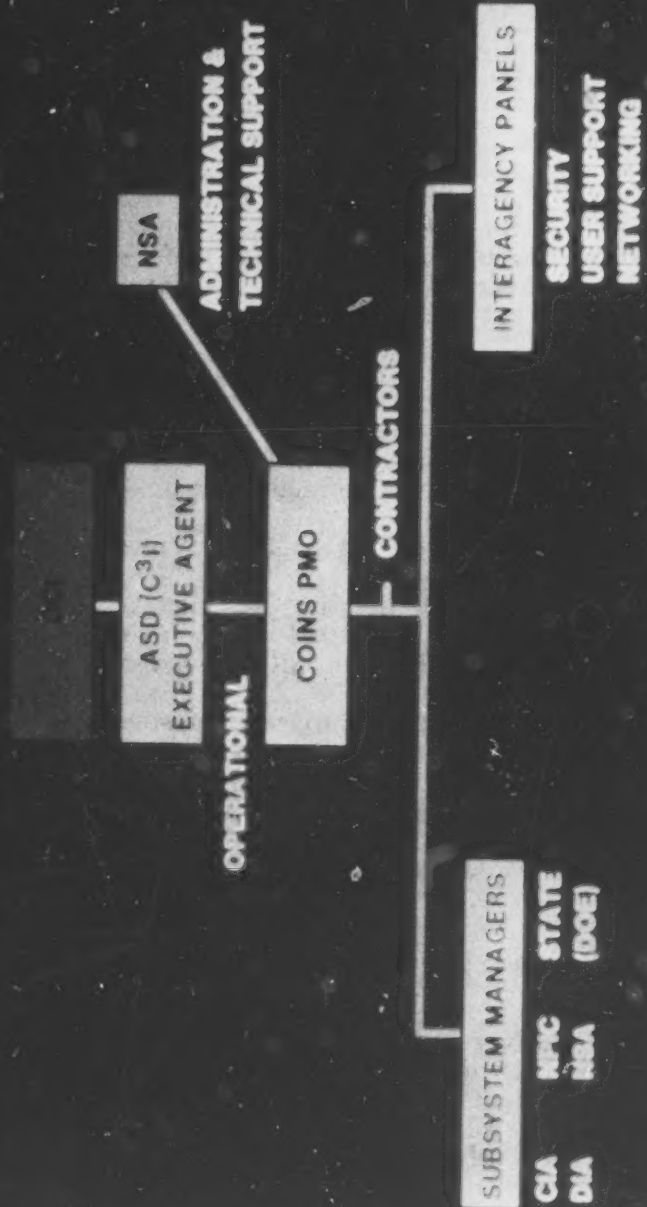


Mr. HICKEN. Now, the User Support Information System [USIS] is a system in which we are installing all of the user aids. We are now servicing somewhere close to 57 different sites or organizations worldwide. We are handling in excess of 80 data bases and the problem is how to train the users to use these facilities and keep them abreast of changes that are going on within the retrieval languages and within the data bases, themselves. So what we are building on the TTRF is a User Support Information System which is available to the users in either a batch or interactive mode.

A file sponsor in either network can update his files or file descriptions, or descriptions about his retrieval languages online. Then users in either network can access this in either a batch or interactive mode, depending upon their capability to retrieve the data they need to determine how to use the information that is available in the network.

[Chart entitled "COINS Management Structure" follows:]

COINS MANAGEMENT STRUCTURE



JULY 78

UNCLASSIFIED

Mr. HICKEN. This is our management structure today. The network operates under the auspices of the DCI. In 1973, after the evaluation of the coins program, the DCI appointed the Assistant Secretary of Defense, Intelligence, and now ASDC³I to be the Executive Agent for the program. Operationally, the COINS PMO is located at NSA, and I report directly to the Assistant Secretary of Defense (Communications, Command Control and Intelligence). NSA provides the COINS PMO with the administrative and technical support as the host agency needed to carry on the program.

You will note that each of the agencies in turn have subsystem managers, and these managers are the individuals in each agency with whom I work and coordinate the networking activities, including NSA. NSA has its own subsystem manager. I do not represent NSA's participation in COINS. That is done elsewhere within the Agency, and I coordinate activities with him just like I would with State, Department of Energy, or any other organization we may be dealing with.

In addition, we have interagency panels set up to handle such discrete things as security, user support and networking problems. Also we have large teams of contractors that work with us in developing and operating the network.

This is our organization management structure that we are using at the present time.

That concludes the formal part of my presentation. I hope it is useful to you.

I couldn't help the other day looking at some of the problems that people are facing, and although the agencies are different, the terms are different, it is essentially the same problem.

Mr. GORE. That is very true.

Thank you for a most impressive presentation. I am very supportive of your system, and, as a member of the Permanent Select Committee on Intelligence, I am supportive of it there as well.

I guess you get a lot of concern expressed to you about the security of the system, with so many access points, but I take it you are well satisfied on that score.

Mr. HICKEN. Yes, very well satisfied on that score.

Mr. GORE. In your opinion, how flexible are the major networks which might be utilized in an emergency? Do they possess a true contingency capability? From your viewpoint, how would you assess them?

Mr. HICKEN. Not in all cases. We only have experience you know with two existing networks. We are looking at interconnecting with at least four other networks within the next 2 or 3 years. Each of these networks will present different kinds of problems to us when we do make the interconnections, and they will offer us a different way.

One of the values you have from internetworking, is that you don't have to drag your own communications facilities to begin expanding. You can use an existing facility and go to a PACOM, like we did using the ARPANET.

ARPANET, of course, is not an operational net in the true sense of the word, but it is a network permitting us to use that facility in an operational vein. It was not built for that kind of an operation, but I think you could use any existing network you wanted. You

should have alternate routes to every path that you are going to take. In fact, we now believe in studies we have conducted, that you should have two gateways between every network at alternate sites.

Mr. GORE. The network is a hard wire system?

Mr. HICKEN. We use satellites.

Mr. GORE. That is linked to satellites?

Mr. HICKEN. That is right, we have satellites and landlines.

Mr. GORE. And they are interchangeable?

Mr. HICKEN. No.

Mr. GORE. Both components are a necessary part?

Mr. HICKEN. Right.

Mr. GORE. In managing the network do you find that the human decision makers become overly dependent upon computerized files?

Mr. HICKEN. No, not yet.

Mr. GORE. How do you avoid that problem?

Mr. HICKEN. I think the analysts use the files but they usually have backup methods for getting data too. They have not relied fully on the automated system. As time goes on and they get more experience with the systems, they will begin to rely upon it more and more. We find that the further you get from the Washington area the more the people rely on the information since it is the only source they have.

You find them relying on it so when we are down temporarily phones ring and people complain and you know they are out there and they really do want service.

Mr. GORE. If you had the option of redoing your system with no limitations on choices imposed by past development, what would you do differently?

Mr. HICKEN. I think the key things today when you look at technology that is emerging you are finding a lot of cable TV systems that are coming into being and the linking of these systems together using satellites as well as crown placed communication facilities, and I think we should move more in that arena, having buildings wired using local cable systems, linking the buildings and the commands together using the satellites for ground based communications. We should be using both of those modes of communications.

Mr. GORE. That is fascinating. When planners speak of linking several networks together during a postdisaster period, when many standing facilities are no longer operating, where should their priorities be placed?

Mr. HICKEN. I don't think—if you have networks—that you want to link together suddenly after a disaster or an emergency. It is not something that you can do after the fact. You have to have it planned before the fact and have the connections made and tested out. To suddenly decide that you want to take two existing networks and plug them together and make them work would be very, very difficult in a short run unless they have had a lot of prior experience working together.

Their protocols are different for interconnecting.

Mr. GORE. So you have to set up the plans ahead of time.

Mr. HICKEN. And exercise it regularly after it is interconnected so that the user of the network and the managers of the network have experiences on sharing across the interface or gateway.

Mr. GORE. Have we passed the point with these highly sophisticated networks where under conditions of extreme duress they could not be replaced by choice with more simple backup systems?

Mr. HICKEN. No. Not at this point in time. We are already looking at replacing our access systems on that ring which started out to be PDP 1134's and 1170's and now we are moving into the ZILOG 8000 category.

So, the price of interface units are drastically falling.

Mr. GORE. It is most impressive and if we could figure out how to use this kind of brilliant system in other areas I think we would be a long ways toward the goal that this inquiry is directed at.

Mr. HICKEN. Yesterday in a number of different speeches they made reference to linking data bases of NOAA, Atlanta together, along with Census and there is no reason why these computer systems could not be linked to the ARPANET.

Mr. GORE. Use the same—

Mr. HICKEN. Same ARPANET. The communications backbone is there. It goes across country. It is unclassified data. Put front end in; link the host processes in and anybody with a dial up phone and terminal could dial up and query you.

Mr. GORE. You have no capacity problem?

Mr. HICKEN. I don't see a capacity problem. You have to ask DCA but they are plugging additional hosts in all the time.

Mr. GORE. We may make that specific recommendation in our committee report.

Mr. HICKEN. It is a simple kind of thing to go ahead and do.

Mr. GORE. That is wonderful. Thank you so much. If I could think of some better questions I think I would probably learn more from you. Maybe we will submit some more questions later on for the record when we figure out what we need to know, because I feel that you know it. Thank you very much for your help today. We appreciate it.

Our next witness is Dr. James W. Morentz, president of Research Alternatives, Inc., Rockville.

Dr. Morentz publishes the nationally known Hazard newspaper.

We are pleased to have you, Dr. Morentz. You can help us a good deal on this inquiry and we are looking forward to hearing from you.

STATEMENT OF JAMES W. MORENTZ, JR., PRESIDENT, RESEARCH ALTERNATIVES, INC.

Dr. MORENTZ. I am happy to be here. It is a topic that is very close to many of the things we have done over the last several years.

Before I begin, I would like to share with you my bias so that you can use it to observe the information I am going to provide for the rest of the testimony. The bias is that unless a consistent policy and program for using information technology in emergency management is developed, 3 years from now, very near term, emergency programs in the localities in the country will not be as well managed as a local barbershop or as a local butcher shop.

Inexpensive computers have made such an impact on small business that even the smallest will have more knowledge and more analytical power at their fingertips than the office that is charged with protecting the entire jurisdiction from catastrophe and leading the community survival from a nuclear attack.

With that as background, I would like to make a couple of observations on these hearings.

The first one is the tremendous scope of emergency management that you have chosen to examine. We have gone from international strategic posture to registering victims at a Red Cross shelter. We have gone from satellite systems to Mr. Allen's trying to get the police and the fire talking together on the same network. We are really talking about two different worlds of emergency management—national crisis management and grassroots emergency management.

As well, we are talking about two different kinds of information capabilities that exist at these levels. At the national level, although we have heard a lot of concerns and complaints about it, we really have the capabilities of instantaneous communication, tailored information analysis, ready access to technology and the information that it holds, and the skills and the people available to use that information.

At the local level where we are talking about the emergency services, fire, police, emergency medical, civil defense, public works, and search and rescue, Mr. Allen's example was even better than in some jurisdictions. In many cases not only are fire, police, and emergency medical services operating on different radio frequencies, but also there is no central point at which they can be mixed to ever interlink or switch them so they can talk together.

The subcommittee is going from ARPANET to the most basic communication problems, where sometimes you are better off with digital smoke signals that Dr. Baker talked of yesterday.

From my view, it is this grassroots emergency management level where the focus and where the greatest need is. That is where response takes place every day, the front lines. As Dr. Hober said yesterday, if anyone is to recover from a nuclear exchange it will begin at the local level.

Given these wide differences between national crisis management and grassroots emergency management, I was drawn to wonder where are the similarities and the differences.

It seems to me that spanning the two points is information packaging. It has been discussed several times. Mr. Baker's 40 bits a second is how do you package information. That is the similarity that spans the national and the local level.

The dissimilarity that separates the two is the access to information technologies. The third piece in this analysis is what is necessary to try and bridge the gap: What is necessary in the form of assistance to help bring the local level up to something that approximates this national level and this national capability?

I would like to hit on these three points. The first one I will summarize is information packaging. It is really what we have been discussing. What has probably been missed in several presentations is, what do we talk about when we mean information for

emergencies? I am going to draw on three different systems we have developed to try and illustrate this.

There are figures in the back of the testimony—several of them—if you have those in front of you. I will talk about three different systems that we developed: The first is called the Lessons Learned System developed for the U.S. Office of Foreign Disaster Assistance. It is a computer-based evaluation system.

The second one, General Ott mentioned that they are using it in Arizona, is the National Emergency Assistance Programs Index. It allows on-line retrieval of information about 300 Federal and national level private sector disaster assistance programs.

The third one is a small, microcomputer-based information package that we are in the process of marketing to local emergency services.

Let's talk first about the Lessons Learned System. The Office of Foreign Disaster Assistance operates in the Agency for International Development. Their job is to provide assistance in the first 60 to 90 days of a disaster. The problem they faced was that people change, but the Office's emergency response did not. There was a lack of an institutional memory for people to know what had happened in past years that could be applied to current disasters.

Our task was to create this institutional memory. I will use one quick case study that is accompanied by the first several figures to illustrate how this information was packaged and used in the Foreign Disaster Assistance Office.

In 1979 Hurricane David swept across the Caribbean and dealt considerable destruction to many of the countries. In particular the Dominican Republic sought aid from the United States, making a request to President Carter for a field hospital—among other things—to provide medical services to victims.

The President thought that sounded like a good idea and passed the request to the Administrator of the Agency for International Development who passed it on to the Office of Foreign Disaster Assistance. The head of OFDA at that time suggested this would be a good chance for the Administrator to see how decisions were made, how OFDA made choices about what they send and where they send it.

He invited the Administrator down, hooked him up with the Lessons Learned System, and this is roughly the scenario that was followed.

Look at figure 1. By simply typing the word "lesson" the computer retrieves this first instruction format that explains what is about to happen. It is accompanied by a whole guidebook but, the screen briefly describes what you need to do in order to get information out.

Pushing a button, you get figure 2, which is a request manual. Focusing at the top on activities undertaken and resources utilized in the past, the head of OFDA typed in the word "hospital" because he was interested in field hospitals.

That entry prompted a series of responses that listed in a few words the experiences that the agency had had in providing hospitals to countries following disasters. Among those listed were the U.S. Army field hospital operations after the Guatemalan earthquake in 1976.

That seems to have been the most similar locale and type of destruction as the Dominican Republic earthquake so they decided to retrieve that one. Pressing one more button they got what appears in figure 3: A brief summary and statistical readout of the evaluative comments that were made following the use of the Army field hospital.

The Administrator quickly saw all that on those 17 different performance characteristics, they pushed over to the left—"the poor and very poor"—and that the summary statement was that the field hospital itself was generally acknowledged to have been a mistake.

You can then probe any one of these 17 categories or take a look at them all to find the reasons behind these evaluative comments that the Administrator saw. Look at figure 4, which is the brief summarization of the reasons given. The first one happened to have considerable persuasiveness with the Administrator because he saw that the reason that the field hospital was given in the first place in Guatemala was because of the Guatemalan familiarity with the field hospital and the personal request by the President.

It had the overtones of the same sort of political rather than pragmatic decision that seemed to be taking place with the Dominican Republic case that they were examining then. Upon further examination—look at figure 5—cost-benefit ratio, midway down the page, showed that the field hospital cost roughly \$1 million and served only 460 patients.

At this point, the Administrator was becoming a little hesitant about the commitment that the President seemed to be making for the field hospital and they turned to what is the last display on Lessons Learned, the recommendations—shown in figure 6. There it became quickly evident that the conditions that are recommended for providing field hospitals—that they have a speedy delivery and that in general they have a smaller, more tailored response—simply could not be met in the Dominican Republic case.

So, the AID Administrator took this information under advisement and the field hospital was not sent.

The point of all this—listing it under my topic of information packaging—is that this was easy to use, readily retrievable, and particularly impressive when you contrast it to the alternative.

The alternative for us was to gather this information by retrieving boxes of files out of deep storage in Suitland, Md. Were it not for the Lessons Learned System, were it not for any additional type of institutional memory, this information would simply be unretrievable.

Mr. GORE. If I could interrupt you there, are you aware of the small field hospital set up by a private group from Tennessee after the 1976 Guatemalan earthquake?

Mr. MORENTZ. There were two or three that went in. There were some package disaster assistance hospitals that were provided by both Red Cross and by State organizations. Some of them tended to be better used than others. The smallness was attractive compared to the Army field hospital that went in with six trucks and tons and tons of equipment.

Mr. GORE. There was one specific case to which I refer, a commune in rural middle Tennessee found out about the severity of

the earthquake by shortwave radio and immediately dispatched a contingent from this commune down to Guatemala. They constructed a field hospital and sent trained medical personnel to staff it and they stayed there for a long period of time and later were commended by the Embassy and the government people there for making a marvelous contribution to the situation.

Throughout they maintained communication with their own base in middle Tennessee by shortwave radio.

Mr. MORENTZ. A good example of radio communications, and that the small, tailored response that seems to work frequently in these international disasters.

The second example that I would like to give to you involves the national emergency assistance program index. This was a project funded a couple of years ago by the Federal Emergency Management Agency and developed by the National Governors' Association. Its purpose was to inventory the programs that are available at a national level to provide assistance to States and localities in predisaster mitigation, preparedness, disaster response, and disaster recovery.

The product of that study was a set of approximately 300 different Federal and national level private sector programs that offer resources to States and localities.

Figure 7 shows a printed version of that. What we have done is develop a computer system that allows for on line retrieval of this information which also is used to generate tapes that are used by the Government Printing Office. Thus, the system is available both in hard copy form and on-line as seen in figures 8 and 9. It is very versatile in that you can approach retrieval from six different indexes depending on the nature of your emergency or the nature of your request. You respond to those by answering questions of whether the emergency phase is something that is important or the type of assistance, or whether declarations are in effect.

In each of these six indexes, then, you go into a whole set of index categories to help you as best as possible to match your particular needs to these 300-plus Federal programs.

A list of the programs that match your categories are then printed out and the individual can further query the computer. It will let you have the full text of the program printed or, if the printed version is available, the user can turn to it.

I will use this to illustrate packaging again because this information is generally unavailable or unpackaged for use by the emergency manager. Many of the programs are on the Office of Management and Budget's Federal assistance programs retrieval system, but the information contained in the FAPRS data base is not that which is most useful to the emergency manager. In designing this format we went to people and said, "What do you need to know about Federal assistance?"

One of the key concerns found was management considerations; what more can I do than just follow the application procedures? What will increase my chances of actually getting aid? We were able to interview people at Federal agencies, on a fairly limited level, to try and develop some of these management considerations about getting aid.

The interesting nature of NEAP comes from three factors. First, it is inexpensive. Typical search for a user now costs on the order of \$5. Second, it is available. It is a nationwide time-sharing system, and virtually anyone with a telephone and a terminal can have access to the data base. Third and most important, it is tailored and packaged information designed for the emergency managers use. That saves the emergency manager time and trouble by getting him to the proper programs and further will save the Federal Government time and trouble in the long run by not having to process applications that are only obscurely directed to that agency.

For the final example of packaging, I want to turn to the small microcomputer system we are currently marketing to local governments. It is called the emergency information system and it has several programs up and running now. One of them, Mr. Vessey, yesterday, of the Red Cross used as an illustration: The National Governors' Association model format for State and local emergency management incident reporting. We already computerized that and are offering it to States now.

It also includes a series of graphic summary displays that help you portray the historical developments of emergency response as well as a procedure for cataloging emergency experts at the local and State level. Thus, you can quickly develop a telephone contact list and know who knows what and how to contact them following an emergency.

Finally, it does a resource inventory, a topic touched on a couple of times today. This resource inventory I want to use as the last example of packaging information.

In figure 10 you see at the top the whole resource listing, and at the bottom the sorted index of resources. The point in using this as an example is that the packaging of information does not have to involve computers for access. The actual use made of this resource inventory resembles a telephone directory. It is far faster, far more familiar to the user to look up a paper record of a community resource than it would be to set up the computer and actually retrieve the information. What do we use the computer for? The computer makes the information better and it makes it more accessible. It does this by indexing and it does it by rapidly updating the information.

The computer is a marvel at sorting alphabetical lists of names or resources or locations. It does this to the resource and provides the kind of a printout that is shown in the bottom of Figure 10.

More than that though the computer is a marvel at helping the understaffed local emergency manager keep the resource list up to date. The program that we have automatically prints out a letter that is sent to everybody on the resource list. It provides the information that is contained in the resource and asks the person to send the letter back with any changes or any update and to confirm that that resource is in fact still available. A key problem that we discovered in talking with local emergency managers was readily solved by this: knowing when the resource list was last updated and updating it as easily as someone can fold the letter and mail it out.

Let's put packaging aside. Packaging, we see, spans from the national level to the local level, important for every use of information.

Let me turn briefly to the topic that divides this crisis management from grassroots emergency management. That is access. Access is simply getting the computer—let's step back—it is actually getting the information however it comes to you. If we had an excellent mail system perhaps that would be the best way to provide information to the local emergency manager. My bias, as I said, is for the technological applications.

Access for localities can be applied or supplied in two different ways. One in time sharing systems and the other in small self-contained computers located in localities. There are advantages to both. One advantage that Congressman Brown yesterday was asking about in the discussion of communications is that the small locally available computer will provide a survivable autonomous unit. Time sharing systems depend on telephone lines, the first thing to go down in a hurricane and certainly the first things that will be destroyed in event of a nuclear attack or any of the more major disasters.

But whatever controversy that might exist between and time-sharing systems or independent local computers is solved by making local computers and time sharing systems communicate with each other to develop networks. The kind of network that is available right now using commercial telephone lines and small computers is illustrated in figure 11. This is the kind of model that the State of Illinois Emergency Service and Disaster Agency and my firm are currently seeking funds for from the Federal Emergency Management Agency to do a demonstration project. It would locate a computer in the State emergency office, and it has four computers in State regional offices, and seven computers in counties and localities.

This is really an illustration that as the computer and communication technologies improve and become lower in cost this kind of network is definitely going to take place.

Now is the time however to start to plan and to put the tools into the hands of local emergency management planners to harvest this technology.

Addressing what I see as the key principle of emergency management, that it is a local responsibility, the task at hand is to build the emergency management information system not the way the emergency management system has been built. That way is to think about the unthinkable and assume that everything else will fall out from it. We have planned at the Federal level for nuclear attack, with the assumption of a trickle down effect to help local government with floods and hurricanes. That has not worked.

The way to plan the information emergency information system in the future is to begin with what happens every day and that is the floods, the tornadoes, the hazardous material spills. Begin to build the local system up to interconnect with a national system, because it is at that local level that the first line of defense for any emergency is going to take place.

How do we go about doing that? Let me look a little to the future and touch on the third topic which is assistance.

I see two different areas for assistance needed to apply information technologies to emergency management. Similarly there are two sources where this assistance can come from. Two forms of assistance needed I see are computer literacy and technological availability.

Computer literacy is exactly what Dr. Baker was talking about yesterday, and what Mr. Allen was talking about today. You must have the people there who can deal with the computers, understand the computers as a tool of emergency management and are able to converse and communicate, and comprehend what the computer is providing. Computer literacy is a skill. It is achievable through training just as written literacy is. Computer literacy is taught in the American educational systems increasingly but for the adult emergency manager, computer literacy is a form of retrofitting, a form of continuing education. The commitment to this continuing education is absolutely necessary to achieve what we have been talking about today.

The second need for information technology assistance lies in—

Mr. GORE. If I could interrupt you, I might note for the record that a group that I chair called the congressional clearinghouse on the future is sponsoring a computer literacy short course for Members of Congress. That is coming up later this year. I agree with your comment on the need for that retrofit. I feel it most acutely myself but excuse me for interrupting. Go ahead.

Mr. MORENTZ. The second area of assistance has to be in technological availability itself. It simply is getting the information management tools into the hands of the emergency managers. Computers for localities I see as a very inexpensive alternative to increased manpower or the worst alternative, decreased preparedness for all the disasters that face the localities.

Turning to sources of assistance, from my vantage point there are two. One is the Federal Government and the other is private business and industries. Federal Governments I really see as both demonstrating and educating for the application of information technology.

Funding a demonstration project in real life applications that are carefully monitored, evaluated, limited periods of performance and carefully defined objectives is one way to show that an investment made by a locality in an emergency management information system is going to pay off in the long run.

The second way perhaps as important or even more important is the Federal Government's opportunity to train. This specifically occurs at the Emergency Management Institute and National Emergency Training Center that FEMA runs.

The Federal Government has the opportunity to train in computer literacy in two different ways. One is training simply on computer applications in emergency management. But then second and perhaps a more insidious way is just utilizing computer-based training techniques whenever possible. That way the 600 to 700 emergency managers—which I think is the number who are being trained each year coming through the Emmitsburg facility—take home with them not only skills in emergency management, but also the beginning of familiarity with touching computers.

The role for the private sector is slightly different. As Dr. Belden suggested earlier, technology itself is a hazard. We see that—in particular with chemical manufacturing plants—while offering tremendous benefits to the community they also increase the risk that a community faces. Probably the same could be said for the hotel and real estate businesses. Without high-rise buildings there would be no high-rise fires for which the local community would have to prepare.

The point is not to denigrate progress but rather to show that business and industry are primary beneficiaries of emergency management. And that a course for the future in applying information technologies is included in the emergency management system the current users of information technology now—hotels have an incredibly complex information-sharing system; chemical manufacturing plants have production lines that are computerized. They are experienced with information technologies.

To begin to bring the private sector into partnership in the emergency management is one goal that can be carried out through sharing of information technologies.

One final example. Dow Chemical has a plant in Midland, Mich., and in 1977 or thereabouts, a chemical release plume went up and they were simply unable to contact the local emergency management authorities in order to get an evacuation started. It ended up not being a damaging release, but Dow Chemical recognized that they had on their own plant a computer warning system and modeling program for wind speeds and wind directions to accurately predict the path of a toxic chemical plume. But their contribution to the community ended at the boundaries of their plant.

So, what they did following that experience was to tie the local emergency management agencies into a direct link to the computer model and direct link to the warning system. The brilliance that existed in the computer technology forecasting that Dow Chemical had is now shared with the community and in the event of a spill, this hopefully would lead the emergency management folks into a better capacity to respond.

Let me conclude by going back to that little warning about the butchers and the bakers. The technologies are there. There will be better technologies in the future and we can sit around and wait for them but the disasters are going to continue to happen.

The first role in computer or applications of information technology has to be with the packaging. It has to begin with identifying what is the information that is useful for the emergency manager.

The future then moves into applying that information packaging into locally tied national networks of information sharers in which the Federal Government, private sector, and the local level can become part of a community of emergency managers that I see structured in large part by the way they share information.

Thank you.

[The prepared statement of Mr. Morentz follows:]

TESTIMONY OF JAMES W. MORENTZ, PhD
 PRESIDENT, RESEARCH ALTERNATIVES, INC.
 BEFORE THE U.S. HOUSE OF REPRESENTATIVES
 COMMITTEE ON SCIENCE AND TECHNOLOGY
 SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
 WEDNESDAY, SEPTEMBER 30, 1981

I come to you today representing a variety of experiences in applying information technologies to emergency management. I am president of Research Alternatives located in Rockville, Maryland. The firm specializes in providing services in the emergency management field. In the past five years we have worked for federal agencies and state governments conducting research about or evaluations of more than 250 different disasters in this country and abroad. The firm publishes a tabloid newspaper, called Hazard Monthly that examines all aspects of natural, manmade, and attack emergencies. We have developed training programs for local emergency managers and have previously contributed to the efforts of Congress through projects for the Congressional Research Service and the Office of Technology Assessment. I, personally, became involved in the emergency management field as the result of a doctoral dissertation for the University of Pennsylvania on the high drought in Sahelian West Africa in the early 1970s.

To begin my testimony, I offer the following observation that I shall return to in my concluding comments. Bear it in mind as my admitted bias in presenting the information you have requested.

I believe that unless a consistent policy and program for using information technology in emergency management is developed, three years from now emergency programs in the local communities in this country will not be as well managed as the local barber shop or butcher shop. Inexpensive computers will have made such an impact on small business that even the smallest will have more knowledge and analytical power at their fingertips than the office charged with protecting the entire jurisdiction from catastrophe and leading the community's survival from a nuclear attack.

The Context of Computer Use in Emergency Management

In examining the topics of testimony for the first two days of these hearings, I have been struck by the two different worlds of emergency management for which roles for information technology are currently being sought. On the one hand, we have the world of national crisis management with capabilities of instant communication, tailored information analysis, ready access to the technology and the information it holds, and skills possessed by crisis management personnel to utilize such information. True, the picture is not entirely rosy at the national level; however, in

contrast with other levels of emergency management the use of information technology is of high quality.

Those other levels which contrast so with national crisis management are, what I call, grass roots emergency management. Here, we are talking about the local emergency services: fire, police, civil defense, emergency medical, public works, search and rescue, and others. While the national capability to effectively use information technology can be belittled, the national capability far exceeds that of the localities. And let us not forget that since the 1950s the front line of emergency management has been the locality--supported by state, and then federal government only when the emergency exceeded the capacity of each successive level of government.

It is at the grass roots of emergency management that survival will be determined. And it is there that the availability of technology and skills for the application of information to emergency management are so lacking.

I, then, paint a picture of a wide gulf between national level crisis management and the grass roots of emergency management. The gulf exists in terms of information technology use. However, it is not a gulf, but a continuum in terms of emergency management responsibilities. There must be an emergency management system that spans national crisis decision-making and local emergency management. That system barely exists today. The role of information technology in the future is to build that effective, national emergency management system.

If we define the goal of using information technology as building a national emergency management system, then we need to look at the two levels that exist today: national crisis management and grass roots emergency management. In this presentation, I suggest that there are three facts that must be recognized in order to bring together the widely differing levels of emergency management:

- First, national crisis management and grass roots emergency management are similar in their needs for information packaging.
- Second, the national and local levels are tremendously different in their access to information technologies.
- Third, the initial step necessary to bridge the gulf that exists between national and local emergency management is assistance in the improvement of skills in using information technologies and access to those technologies.

In the following presentation, I will detail these three components: information packaging, technology access, and needed assistance. But before turning to the discussion, let us make certain of our definitions.

By packaging, I mean the use of information technology in expanding the utility and availability of accurate, up-to-date information. The focus here is on creating useful information for whatever level of decision is necessary.

By access, I mean expanding the opportunity to use information through

information technology. The focus is on getting information technology into the hands of users in the emergency management field.

And by assistance, I mean the aid necessary to achieve both improved packaging and wider access. The focus is on the role of government and the private sector in demonstrating the value of technology and improving the skills of potential users.

PACKAGING

Examples of packaging information through computers to produce a more useful way of reviewing the information consist of three systems developed by my firm, Research Alternatives through its emergency information division:

- The Lessons Learned System of the U.S. Office of Foreign Disaster Assistance is a computer-based evaluation system that provides an institutional memory of U.S. performance in providing international disaster aid.
- The National Emergency Assistance Programs Index allows the online retrieval of information about more than 300 federal and national private sector assistance programs. It is a time-sharing system available from normal telephones anywhere.
- Emergency Information is a small microcomputer-based proprietary information management package currently being marketed to local government emergency services---fire, emergency medical, civil defense---to automate their damage assessment, resource inventory, emergency contact lists, and statistical analysis of their performance.

The Lessons Learned System

The Lessons Learned System was developed over three years under contract to the U.S. Office of Foreign Disaster Assistance of the Agency for International Development. The purpose of the system was to create an institutional memory of the office of their experiences in providing aid after disasters. The need for this institutional memory was clear: personnel changed fairly frequently, the director is a presidential appointee and in five years the office had four different directors and at least three different acting directors. Yet, amid all this personnel change, the functions of the office are relatively uniform: to provide the assistance necessary in the 60-90 days following a disaster to relieve damage and human suffering.

Thus, using information technology and human analytical skills to create an institutional memory was an appropriate undertaking. Let me illustrate the importance of the Lessons Learned System as a tool for information packaging with one example.

In August of 1979, Hurricane David swept across the Caribbean dealing death and destruction to several of the islands, in particular, the

Dominican Republic. The government made a request to the U.S. President for a field hospital to help provide medical services to victims. The President was inclined to send the field hospital and asked the Administrator of the Agency for International Development to see to it. When the request came to the Office of Foreign Disaster Assistance (OFDA) the acting director at that time saw this as an opportunity to use the Lessons Learned System as a decision aid.

The AID Administrator was invited to the offices of OFDA to see how decisions of this type were made. The following series of illustrations show what the head of OFDA showed the Administrator.

By typing the word "LESSON" OFDA's institutional memory comes online as part of a minicomputer using television-like display screens and printers for hardcopy. The word "LESSON" results in the display seen in Figure 1. The brief instructions for using the system are, of course, supplemented with a complete Users' Guide.

Figure 2 shows the next display, a Request Menu where the user enters the activity undertaken or resource utilized about which the user wants information. The information retrieved can be restricted by the type of disaster agent (earthquake, hurricane, etc.), the region or country, or the within country locale (urban, rural, countrywide). In the case of the AID Administrator's interest in field hospitals, the activity/resource shown in the figure is "HOSPITAL" in "LATIN AMERICA."

The result of entering this information is a listing of all occurrences of the activity/resource on the Lessons Learned System. From this list, the user can then select appropriate for detailed examination. Appearing on the list presented to the AID Administrator was "US ARMY FIELD HOSPITAL OPERATIONS" in the 1976 Guatemala earthquake.

Returning to the Request Menu, a single four-digit number was entered and a button pressed to produce the display shown in Figure 3, an evaluation and summary statement on field hospital operations. The thrust of this summary is that field hospitals are costly and usually do not arrive quickly enough to provide immediate aid. The majority of evaluations were in the poor and very poor range. In the case of Hurricane David, the AID Administrator's enthusiasm for the field hospital began to erode.

Figure 4 shows the next step the AID Administrator and the head of OFDA took: To look at the detailed Reasons for such poor performance. Any one of the 17 performance characteristics that appear on the summary can be retrieved individually. Figure 4 shows comments on all characteristics.

For the AID Administrator, the reason for the delivery of the field hospital in Guatemala, that the government knew about it and pressured the U.S., was similar to the Hurricane David request coming directly from the White House. Reviewing the relatively poor utilization of the hospital, and (Figure 5) the high cost, the AID Administrator began to question the delivery of the field hospital.

When the head of OFDA and the Administrator finally turned to the last of the displays on Lessons Learned, Recommendations, it had become clear

that the field hospital could be a mistake. The General Recommendations (Figure 6) showed the conditions under which a field hospital could make a contribution: speedy delivery and smaller, tailored response. Under the circumstances of Hurricane David, the AID Administrator agreed that those conditions could not be met. The field hospital was not sent.

This single case study becomes an even better example of the importance of packaging information when we recall the procedure my firm went through to gather the evaluative comments for the nearly 1000 lessons learned that now exist. Our review of documents ranging back to the early 1970s required retrieval of boxes of files from deep storage at Suitland, Maryland. For the AID Administrator, or any new personnel of OFDA, the institutional memory of the Guatemala earthquake was virtually inaccessible. Now, summarized and retrievable on OFDA's computer, the Guatemala earthquake continues to live as a lesson for the future.

National Emergency Assistance Programs Index

The National Emergency Assistance Programs Index provides a second, different, illustration of packaging information for emergency management. This tool has been available for use in federal agencies and, selectively, at the state level to retrieve information concisely summarized on federal and national private sector emergency assistance programs.

The project was funded by the Federal Emergency Management Agency and developed by the National Governors' Association. My firm worked under contract to NGA.

The origin of the project was to develop an inventory of programs that provide assistance in the pre-disaster phases of prevention, mitigation, and preparedness, disaster response, and recovery. The need was based in the inappropriateness and incompleteness of the descriptions of existing federal programs (specifically the Federal Assistance Programs Retrieval System of the Office of Management and Budget). To date, more than 300 programs have been catalogued, annotated, and computerized for retrieval and electronic typesetting.

Figure 7 shows the format of a NEAP description, including purpose, authority, type of assistance, applicant eligibility criteria, and application procedures. This version was electronically typeset by the Government Printing Office from tapes made by Research Alternatives. These same computer tapes form the basis of an online, time-sharing retrieval system accessible from any telephone in the country.

Figure 8 shows the six indices that exist for NEAP. Using one or more of these, the user can match his or her emergency-related needs and narrow the number of programs displayed by the computer. After selecting the appropriate indices, categories of each index are displayed. One page of categories is shown in Figure 9.

After selecting as many or few of the categories match the needs of the emergency conditions, the computer prints a list of all matching federal and national private sector programs. The user can then use either

the printed version of NEAP (as shown in Figure 7) or can request a full-text printout from the computer.

The vitality of NEAP comes from three factors:

- First, the information is available nowhere else as completely and as tailored to the emergency professional. Simply, it is packaged for maximum utility.
- Second, it is inexpensive. A typical search costs a user only three to five dollars. Thus, it can be widely used.
- Third, it is available. Anyone with a computer terminal can have access to the data base.

But, most important, in my view, is NEAP's tailored, packaged information designed for emergency managers. The system expands the capability of the emergency professional to look across a wide range of possible sources of assistance—not just money but information, skills, in-kind services, etc. Furthermore, it improves the local and state manager's ability to pick appropriate sources of assistance, thus minimizing effort spent on fruitless searches and effort wasted by program personnel reviewing useless applications.

The Disaster Information System

This third example of information packaging is included to show how inexpensive computer systems can serve emergency needs and to show how packaging does not always mean automating information use.

We are currently marketing to state and local governments and private sector emergency-related organizations a microcomputer that manages emergency information. It helps report damage assessments by automating a format promoted by the National Governors' Association as a model for state and local damage reporting. It provides graphic displays of emergency statistics that are useful in describing the emergency program and efforts over a period of time, such as, amount of damage, number of miles driven by emergency services, overtime hours, and a modification of the lessons learned discussed above. The basic Disaster Information system also helps localities do resource inventories and develop and update emergency contact lists of experts.

It is the resource inventory that I want to use as a final example of information packaging. A sample of the resource inventory display is shown in Figure 10. Included are sorted summary indices and full descriptions of the resources.

The point to be made about the resource inventory is that retrieval, the packaging, does not involve the computer. Rather, the computer is a tool for packaging. The actual use of the inventory resembles a telephone directory. It is far faster, and more familiar to the user, to look at the paper record of the community's resources than it would be to set up the computer and retrieve the information.

Of what use is the computer, then?

The computer makes the information better and more accessible. It does so by comprehensively indexing the information and readily updating it.

The actual format and content of the resource listing shown in Figure 10 differs little from that possessed by emergency services around the country. However, it is virtually certain that the listings in emergency services are difficult to access and out of date. This is where the computer performs service to the emergency professional.

The computerization of the emergency resource list lends itself to rapid sorting and indexing of the resources. Two available methods of indexing are illustrated in Figure 10. Thus, when the emergency manager turns to his or her resource list, it is to a well-sorted index. As well, it is to a paper document as familiar as a phone book. The ease of access and familiarity will lead to improved use of the resource inventory.

Similarly, update can be as frequent as desired at a far lower level of effort than ever before. With a single command, a letter can be sent to all resource contacts asking them to confirm the accuracy and continued availability of the resource or make changes. Thus, when the emergency manager turns to the resource inventory, it is with the knowledge that an accurate inventory exists.

ACCESS

As we have seen above, the packaging of information is a need shared by both national crisis managers and grass roots emergency managers. In looking to the role of information technology in emergency management, improved packaging is a bridge across the disparate capabilities of national and local level emergency professionals.

Separating the national and local level, in contrast to packaging which is a common need, is access to emergency information and information technologies.

This part of my presentation consists of thoughts on getting information technology into the hands of emergency users.

Let me state my bias in this matter: I believe those most in need of improved access to information technology are the emergency services in jurisdictions across the country. The fire, police, civil defense, emergency medical, rescue, public works, and other emergency professionals from states, to counties, to councils of government, to municipalities, towns, and townships. These services are the front lines of emergency management. In any national emergency, from an earthquake, to a hurricane, to a terrorist incident, to nuclear attack, survival will be carried out by

these emergency services.

There are two approaches: (1) time-sharing systems and (2) self-contained computers in localities. Time-sharing have the advantage of access to wider amounts of diverse information at a lower initial cost. Dedicated, locally owned computers have the advantage of offering support services, inexpensively across time, for not just information gathering and analysis, but information management. While time-sharing will provide information local computers will allow locally generated and analyzed information. That is, wider use of the computer to help day to day and crisis management.

The answer to whatever controversy may exist between local computers and time-sharing systems is simply to make local computers communicate with other computers. Information can be obtained from a wide variety of diverse sources (through networking) but, the smallscale, routine tasks for which the computer is well suited to an emergency office (as an office like any other office) would be available on the local computer, including wordprocessing, accounting, etc.

An additional factor in favor of the locally owned communicating computer is its use in emergencies. A time-sharing computer is dependent on telephone lines for access to information. A locally owned computer is independent of telephone lines and can operate on the emergency generator existing in many emergency offices. Whatever emergency use is made of the computer will not be disrupted by the emergency itself.

This kind of a distributed network is illustrated in Figure 11, which shows a model for which the State of Illinois Emergency Services and Disaster Agency is currently seeking funds for a demonstration project.

As computer and communications technologies improve and become cheaper in cost, these types of networks will abound. It is my view that the focus for the future should be on adapting the present and coming advances in hardware technology to the needs of emergency management. Plans need to be laid that will allow planners in emergency management to harness the technology by addressing a primary principle of emergency management: Emergency management is a local responsibility. Therefore, development efforts should be directed to supporting localities with information technology.

NEEDED ASSISTANCE

The assistance needed to enhance the use of information technology lies in two areas. The assistance, similarly, can come from two sources.

The assistance needed to improve the role of information technology in emergency management consists of (1) computer literacy and (2) technology availability.

Computer literacy is, simply, understanding the computer as a tool of

emergency management. That is, being able to converse, communicate, comprehend with the computer as a tool of information management and analysis. Computer literacy is a skill, achievable through training, just as written literacy is. Computer literacy is increasingly taught in the American educational system. For the adult emergency manager, computer literacy is a form of retrofitting---continuing education. The commitment to this continuing education is necessary.

Technological available is, simply, getting the tools into the hands of emergency managers. The essence of this need is a financial one---not a happy topic in these budget cutting times. But, computers for localities are inexpensive when the alternatives are considered: increased manpower or, the worst alternative, decreased preparedness for natural, manmade or nuclear attack disasters.

Turning to the sources of assistance, there are two from my vantage point: (1) the federal government and (2) private business and industry.

The federal government's role in expanding the application of information technology to emergency management is one of demonstration and education. The Federal Emergency Management Agency needs to selectively undertake the funding of demonstration projects of technologies applied to emergency management. These projects need to be real-life applications, carefully monitored and evaluated, with limited periods of performance, and defined and measurable objectives.

Built into every demonstration project must be an information dissemination component that does two things. First it shares information among participants in the demonstration project so that the participants, themselves, can contribute to the refinement of the project. Second, dissemination of information must take place to other interested groups or individuals---those who monitor the demonstration project to make their own decisions about using information technology in their own jurisdictions.

The federal government must also train; it must contribute through its emergency training programs to computer literacy. It can do this both by training about computer applications in emergency management and by utilizing computer-based training techniques wherever practicable. The federal government must, through both demonstration and training, express the inherent value and contribution of information technology to emergency management.

The role of the private sector, specifically business and industry, is to begin to contribute to improved emergency preparedness. Business and industry are, in part, the recipients of the benefits of emergency management. Without the hotel and the real estate businesses, high-rise fires would require little attention from the emergency manager. Chemical manufacturing plants, while benefitting the economic well-being of the community, add to the risk that must be managed by emergency services. It is a basic premise of emergency management that without a risk, preparedness can be minimal. It is time for a movement to occur that constructively begins to include business and industry in emergency management planning.

The role of business and industry, therefore, is to become part of the

emergency management community. This is especially possible in the use of information technologies. One excellent example is the Dow Chemical plant in Midland Michigan. Following a chemical plume release and the subsequent lack of preparedness demonstrated on the part of the local officials, Dow contributed to expanding the warning system of the community. This included direct links to the Dow computer which models plume paths, thus aiding the jurisdiction in making better evacuation decisions. Industry and local government worked hand-in-hand for better emergency preparedness.

CONCLUSION

Let me return to the admonition made at the beginning: Unless a consistent policy and program for using information technology in emergency management is developed, three years from now emergency programs in the local communities in this country will not be as well managed as the local barber shop or butcher shop. Inexpensive computers will have made such an impact on small business that even the small will have more knowledge and analytical power at their fingertips than the office charged with protecting the entire jurisdiction from catastrophe and leading the community's survival from a nuclear attack.

Thus, the role of information technology in emergency management begins, first, with the ability of computers and communications to package information and share it widely.

The future lies in expanded use of computers locally, tied into networks of information sharers.

The future can be developed systematically through training and expanded access to computer technology, both of which are possible financially when the roles of the federal government and the private sector are defined as partners with grass roots emergency managers.

FIGURE 1

```

OFFICE OF FOREIGN DISASTER ASSISTANCE
LESSONS LEARNED SYSTEM

welcome to THE LESSONS LEARNED SYSTEM. It was designed to create
an institutional memory for OFDA by evaluating the performance of
U.S. Government international disaster relief efforts.

System use is explained in instructions on the screen. A single
"Request Menu" will lead you through five different displays:

--ACTIVITY/RESOURCES IN FILE      HINT: Enter ACTIVITY/RESOURCES
--ACTIVITY/RESOURCE LIST          without word endings s, es,
--SUMMARY DISPLAY                 ing, etc., for best results.
--REASONS DISPLAY                 Other than that, type normally
--RECOMMENDATIONS DISPLAY         and follow the directions.

Don't worry, if you make a mistake, the computer will tell you.

THE LESSONS LEARNED SYSTEM was developed by RESEARCH ALTERNATIVES
under contract to the U.S. Office of Foreign Disaster Assistance.

To proceed to REQUEST MENU, push RETURN.

```

```

**** LESSONS LEARNED SYSTEM ****
REQUEST MENU

*** TO DISPLAY
ACTIVITY/RESOURCES ON FILE ... ENTER ANY OR ALL OF THE FOLLOWING,
THEN PRESS DISPLAY KEY F1 (TOP ROW, LEFT)

ACTIVITY/RESOURCE? HOSPITAL
AGENT?
REGION OR COUNTRY?
LOCAL?
DISASTER NUMBER? 1      11      11      11      11      11
                  1      11      11      11      11      11

*** TO DISPLAY
ACTIVITY/RESOURCE LIST ... PRESS DISPLAY KEY F2 (A/R ON FILE MUST BE RUN FIRST)

*** TO DISPLAY
SUMMARY OR              (1) ENTER LESSONS LEARNED          (2) PRESS DISPLAY KEY
REASONS OR              NUMBER AND (OPTIONALLY)          F3 FOR SUMMARY DISPLAY
RECOMMENDATIONS ...     PERFORMANCE CHARACTERISTIC      F4 FOR REASONS DISPLAY
                        LESSONS LEARNED NO.?              F5 FOR RECOMMENDATIONS
                        PERF. CHAR.?

<<PRESS CANCEL ANYTIME TO TERMINATE THE LESSONS LEARNED SYSTEM>>

```

FIGURE 2

FIGURE 3

8/25/25	*****	ACTIVITY/RESOURCE	*****	11:25:22		
EARTHQUAKE		U.S. ARMY FIELD HOSPITAL OPERATIONS				
GUATEMALA						
COUNTRYWIDE						
76021 -1044						
*** EVALUATION ***						
	VP	P	N	Q	VG	
DECISION	1	1				Sending the field hospital was generally acknowledged to be a mistake. It was costly and served relatively few people. It was inadequately supplied with materials and personnel for earthquake assistance which is dominated by orthopedic injuries. In general, medical aid is required so quickly that it must be the responsibility of the local government. The concept of sending aid to victims rather than transporting them long distances continues to be accepted as good
UTILIZATION	1	1				
TIMELINESS	1					
CONTROL	2					
COORDINATION	1					
INFORMATION	2	1				
SUPPLY						
DISTRIBUTION						
FULL NEEDS		2	1			
MAINTENANCE/MONITORING	1					
QUANTITY/DUPLICATION						
TECHNICAL QUALITY	1	1				
SELF-HELP INCENTIVE						
COST/BENEFIT RATIO	2	1				
EFFORT/EFFECT RATIO	1	1	1			
LONG-TERM UTILITY	1					
ACHIEVE OFDA GOALS	1					

8/25/25	*****	ACTIVITY/RESOURCE	*****	11:36:27
EARTHQUAKE		U.S. ARMY FIELD HOSPITAL OPERATIONS		
GUATEMALA				
COUNTRYWIDE				
76021 -1044				
*** EVALUATION ***				
REASONS				
DECISION				
NEUTRAL		Guatemalan President Laugerud specifically requested the field hospital (he had U.S. military training) so OFDA really couldn't refuse (1989)		
POOR		Bad decision because there was confusion in USC ast to just what a field hospital was; for example, no one in Guatemala knew a field hospital came with its own transportation (1999)		
UTILIZATION				
POOR		Initial request was for minor trauma and surgery for 3000 patients for 15-30 days; but only 250 surgical cases were handled in 7 days of operation (5005)		
NEUTRAL		Deployment of field hospital set a precedent for bringing assistance to victims rather than having victims travel long distances for aid (1021)		
TIMELINESS				
POOR		Paramedics arrived too late to help with victims (1024)		
POOR		Excessive time was devoted to meeting fuel requirements once the field hospital was on site in-country (5004)		

FIGURE 4

FULFILL NEEDS

- 1 POOR GUS airlifted victims to the hospital who did not want to leave their families (1999)
- 1 POOR The hospital failed to include a cast man and plaster cast equipment, therefore, many orthopedic patients were poorly served (5004)
- 1 NEUTRAL Presence of the hospital permitted other local health facilities to "get their feet back on the ground" and avoid huge overcrowding (1021)

MAINTENANCE/MONITORING-

- 1 V POOR Fuel for the hospital was at a minimum for 4 days because hospital did not come equipped with tanks or drums for transport of fuel; all had to be borrowed locally (5004)

QUANTITY/DUPLICATION

- 1 NEUTRAL Triage system set up in msa area with medical teams from other nations; several smaller field hospitals would have been better (1989)

TECHNICAL QUALITY

- 1 V POOR The field hospital was not really tailored to the specific disaster needs of earthquake victims, particularly it has poor and inadequate orthopedic capability (5004)
- 1 POOR Field hospital personnel lacked adequate language capability to work comfortably with victims (1024)

SELF-HELP INCENTIVE

- 1 GOOD Sending the field hospital to site prevented a refugee problem by keeping people near villages where they could continue to use their own existing resources (1021)

COST/BENEFIT RATIO

- 1 V POOR The field hospital performed far too few services to merit the logistical problems overcome and the cost of sending it (1021, 1021, 1024)
- 2 POOR
- 1 POOR \$1 million : 460 patients (1989)

EFFORT/EFFECT RATIO

- 1 POOR Discovering a local source and borrowing drums and tanker to transport fuel was time-consuming effort which could have easily been avoided (5004)
- 1 NEUTRAL Demonstration of U.S. presence; C. Bherhorst felt that the field hospital did a very good job and did not represent overkill (1989)

SINGLE MOST IMPORTANT FACTOR

- 1 NEUTRAL Information sharing; more coordination or relative usefulness of hospital of that size to the task might have altered decision (1989)
- 1 V POOR The hospital was too sophisticated; personnel did not speak local languages; there was no appropriate orthopedic team to treat the many fractures (1999)
** END

FIGURE 5

81/09/25 ***** ACTIVITY RESOURCE ***** 11:18:46
 EARTHQUAKE U.S. ARMY FIELD HOSPITAL OPERATIONS
 GUATEMALA
 COUNTRYWIDE
 76021 -1044

***** RECOMMENDATIONS *****

GENERAL

Disasters create special requirements for field medical assistance, including fuel, transport, and specialized medical needs. These should be anticipated and planned for in cooperation with Department of Defense. (5004)

Either smaller units or a more streamlined field hospital should be developed for disaster response. (1021, 1989)

OFDA should focus on a policy pertaining to the USC role in medical assistance. Because lives must be saved in the first 24-36 hours, when life-saving facilities must be provided on an extremely fast basis. The other alternative is to provide assistance for care of the less seriously injured in the 2 day to 2 week period following the disaster. This would require somewhat less prompt response and a different form of assistance. (1024)

DECISION

Smaller medical team should be sent in the future. A field hospital is "too much" for the job. More data should be collected before a decision is made, but by then the use of the field hospital would have lessened (1999, 9999)

OFDA should examine and concur in all DOD-sponsored health assistance. (1024)

UTILIZATION

Primary medical responsibility should lie with the host/victim government. (1024)

TIMELINESS

Helicopter support and paramedics are necessary only in the 24-36 hour life-saving period and should not be deployed later. (1024)

INFORMATION

A process should be created to inform and have verified the anticipated types of injuries in different disasters. These should then be matched with the field hospital's emergency operations plan for meeting special needs of particular disasters. (5004)

Better record keeping is necessary at the hospital in order to help reunite families with victims who were airlifted to the hospital. (1021)

FIGURE 6

120:100

120:100

INTERIOR, UNITED STATES DEPARTMENT OF THE

NAME OF PROGRAM:

SEARCH AND RESCUE

PURPOSE OF PROGRAM:

To provide a supportive role for national, state, regional, and local search and rescue (SAR) operations or lead role for same on Bureau of Land Management administered lands.

ORGANIZATION PROVIDING:

United States Department of the Interior (DOI)
Bureau of Land Management (BLM)
DIVISION OF FIRE AND AVIATION MANAGEMENT

ASSISTANCE:

Use of manpower, facilities, and equipment.

ELIGIBILITY:

BLM operates in the eleven westernmost states of U.S. and Alaska.

APPLICATION PROCEDURE:

- (1) Each district and state office of BLM is responsible for preparation of SAR plan for its public lands;
- (2) All BLM offices have designated one individual and one alternate as responsible for handling SAR program;
- (3) The district or state office of BLM can be directly contacted by telephone when assistance is needed for a SAR emergency.

MANAGEMENT CONSIDERATIONS:

- (1) Under concept of "closest available forces", BLM provides immediate response in order to save lives;
- (2) BLM is restricted to using only manpower and facilities at hand, when responding to a SAR emergency;
- (3) No funds are available from BLM, however, BLM covers costs for its manpower and equipment through its own program funds;
- (4) BLM may negotiate reimbursable cooperative agreements or contracts to provide service, using SAR emergency funds, if area response capability is not adequate.

FUNDING:

BLM programs funds for salaries and expenses: Approximately \$100,000 each year for SAR.

AUTHORIZATION:

Federal Land Policy and Management Act of 1976
Pub. L. 94-579, 90 Stat. 2743

INFORMATION SOURCE:

BLM state and district offices (See Appendix B).

9/80

NATIONAL OFFICE CONTACT:

Mr. Jim Richardson
Chief
Division of Fire and Aviation Management
BLM
Department of the Interior
Washington, D.C. 20240
(202) 343-7964

CLEARANCE DATE: Autumn 1979

CORRESPONDING OMB NUMBER: Not applicable

FIGURE 8

1. FOR WHICH EMERGENCY PHASE DO YOU SEEK ASSISTANCE?
2. FOR WHAT TYPE OF EMERGENCY DO YOU SEEK ASSISTANCE?
3. WHAT TYPE OF ASSISTANCE DO YOU NEED?
4. IN WHAT SUBJECT CATEGORY DO YOU INTEND TO UTILIZE ASSISTANCE?
5. WHO WILL BE APPLYING FOR ASSISTANCE?
6. WHICH DECLARATIONS OR DESIGNATIONS ARE IN EFFECT?

1. ANIMAL PLANT DISTRESS
 2. AIRCRAFT DISTRESS
 3. BOAT DISTRESS
 4. BUILDING DISTRESS
 5. COMMERCIAL DISTRESS
 6. CONSTRUCTION DISTRESS
 7. CRAFT DISTRESS
 8. CRAFT DISTRESS
 9. CRAFT DISTRESS
 10. CRAFT DISTRESS
 11. CRAFT DISTRESS
 12. CRAFT DISTRESS
 13. CRAFT DISTRESS
 14. CRAFT DISTRESS
 15. CRAFT DISTRESS
 16. CRAFT DISTRESS
 17. CRAFT DISTRESS
 18. CRAFT DISTRESS
 19. CRAFT DISTRESS
 20. CRAFT DISTRESS
 21. CRAFT DISTRESS
 22. CRAFT DISTRESS
 23. CRAFT DISTRESS
 24. CRAFT DISTRESS
 25. CRAFT DISTRESS
 26. CRAFT DISTRESS
 27. CRAFT DISTRESS
 28. CRAFT DISTRESS
 29. CRAFT DISTRESS
 30. CRAFT DISTRESS
 31. CRAFT DISTRESS
 32. CRAFT DISTRESS
 33. CRAFT DISTRESS
 34. CRAFT DISTRESS
 35. CRAFT DISTRESS
 36. CRAFT DISTRESS
 37. CRAFT DISTRESS
 38. CRAFT DISTRESS
 39. CRAFT DISTRESS
 40. CRAFT DISTRESS
 41. CRAFT DISTRESS
 42. CRAFT DISTRESS
 43. CRAFT DISTRESS
 44. CRAFT DISTRESS
 45. CRAFT DISTRESS
 46. CRAFT DISTRESS
 47. CRAFT DISTRESS
 48. CRAFT DISTRESS
 49. CRAFT DISTRESS
 50. CRAFT DISTRESS
 51. CRAFT DISTRESS
 52. CRAFT DISTRESS
 53. CRAFT DISTRESS
 54. CRAFT DISTRESS
 55. CRAFT DISTRESS
 56. CRAFT DISTRESS
 57. CRAFT DISTRESS
 58. CRAFT DISTRESS
 59. CRAFT DISTRESS
 60. CRAFT DISTRESS
 61. CRAFT DISTRESS
 62. CRAFT DISTRESS
 63. CRAFT DISTRESS
 64. CRAFT DISTRESS
 65. CRAFT DISTRESS
 66. CRAFT DISTRESS
 67. CRAFT DISTRESS
 68. CRAFT DISTRESS
 69. CRAFT DISTRESS
 70. CRAFT DISTRESS
 71. CRAFT DISTRESS
 72. CRAFT DISTRESS
 73. CRAFT DISTRESS
 74. CRAFT DISTRESS
 75. CRAFT DISTRESS
 76. CRAFT DISTRESS
 77. CRAFT DISTRESS
 78. CRAFT DISTRESS
 79. CRAFT DISTRESS
 80. CRAFT DISTRESS
 81. CRAFT DISTRESS
 82. CRAFT DISTRESS
 83. CRAFT DISTRESS
 84. CRAFT DISTRESS
 85. CRAFT DISTRESS
 86. CRAFT DISTRESS
 87. CRAFT DISTRESS
 88. CRAFT DISTRESS
 89. CRAFT DISTRESS
 90. CRAFT DISTRESS
 91. CRAFT DISTRESS
 92. CRAFT DISTRESS
 93. CRAFT DISTRESS
 94. CRAFT DISTRESS
 95. CRAFT DISTRESS
 96. CRAFT DISTRESS
 97. CRAFT DISTRESS
 98. CRAFT DISTRESS
 99. CRAFT DISTRESS
 100. CRAFT DISTRESS

FIGURE 9

RESOURCE: Heavy Equipment (Dump trucks; Graders)
 NUMBER: 18
 SKILLS/CAPABILITIES: Excavation; debris removal
 TRAINING/EXPERIENCE: Used extensively in Hurricane Betty
 LOCATION: Towson
 ADDITIONAL RESOURCES REQUIRED: Drivers; skilled operators
 PRIMARY CONTACT: Albert King (K & R Const.)
 ADDRESS: 4100 Janeway Rd.
 Bedford MD 30511
 PHONE: 305-414-0966
 HOME ADDRESS: 833 West Wooddale Ave.
 Towson MD 30521
 PHONE: 305-744-4145
 ALTERNATE CONTACT: Richard Hennessey
 PHONE: 305-221-1416
 HOME PHONE: 305-221-2885
 AUTHORITY: Letter of Understanding; 6/4/80
 COST/COMPENSATION: \$35/hr trucks; \$41/hr graders
 DATE CONFIRMED: 1/4/81

HEAVY EQUIPMENT

Highway Dept/Jack Bryan 305-369-2948
 Ace Trucking/Harry Lee 212-378-2980
 Bell Construction/Mr. Dever 305-529-3631
 U of Maryland/David Deldorf 305-567-9090
 Franklin Co./J.F. Franklin 212-479-2947

ROAD REPAIR

Franklin Co./J.F. Franklin 212-479-2947
 Asphalt Contr./Mr. Lester 305-274-3652
 Tonnage Stone/Lee Hanks 305-386-3614

TEMPORARY SHELTER

Red Cross/Joyce Sever 305-283-3846
 Mannonite/L. Kayser 305-374-2965
 School Dist/Sup. Williams 305-478-0754
 First Baptist/Rev. Smythe 305-462-5670

Resource Inventory Sorted By Type Into a
 Telephone Contact List.

FIGURE 10

Mr. GORE. Thank you very much. Your testimony has been right on point. I certainly do appreciate it.

You have produced a handbook, I understand, for FEMA, called *The Emergency Manager: An Orientation to the Position*.

Is that correct?

Mr. MORENTZ. Yes. It is a home study course. It is the first training piece that a local emergency manager gets.

Mr. GORE. What kind of user reaction have you had to this?

Mr. MORENTZ. It has yet to be published by FEMA formally. In our pilot test we distributed around 300 copies and made subsequent revisions according to that.

In general, we got a very favorable reaction to it. In large part it has a very new content introducing the ideas of comprehensive emergency management, rather than civil defense as the total occupation, so there are a lot of new ideas that we are throwing at people as a result of the amalgamation of FEMA into a single agency.

Mr. GORE. We want to make recommendations to FEMA and the White House and the appropriate committees of the Congress that will encourage the greater use of information-handling capabilities enhanced by the new technologies now available in the management of emergency situations.

If you were this subcommittee, what recommendations would you make?

Mr. MORENTZ. Probably the first one would be to get a grip on what is available within FEMA itself, despite the comment made by Mr. Campbell yesterday that they have undertaken a review and hopefully that will solve the problem. But the diversity that is in FEMA is not, I don't think, a strength. It is a weakness. The diversity of their information could well become a strength, but because it is diverse there is no sharing and people are largely unaware of what is available.

To take that a second step would be to identify what is available and use it. The national emergency assistance program index that I talked about—maybe it is out of business by now—it was running out of funding today. As of yesterday a policy decision had not been made about what to do with it. But, it has been available and on line for about the last 9 months and again a policy decision just was not forthcoming on how to disseminate that information. So, we have had what I consider a wealth of information that would assist any community preceding or following a disaster. It has been used exclusively by five Federal agencies and two or three States on a pilot basis.

Mr. GORE. Any others?

Mr. MORENTZ. I would reiterate the idea of training that I mentioned, and supporting demonstration projects, because there are systems like mine that for a relatively low cost could be demonstrated and monitored to actually see how well information technologies serve the States and localities.

Mr. GORE. Well, I appreciate your appearance here today. I could ask a number of other questions but we have run way overtime and we have to move it along.

Thank you so much for an excellent contribution today.

Our last witness is Dr. Robert Kupperman, executive director of the Center for Strategic and International Studies at Georgetown University.

Dr. Kupperman, we are most pleased to have you join us today. Without objection the entire text of your statement will appear in the record and we would like to hear from you.

**STATEMENT OF ROBERT KUPPERMAN, EXECUTIVE DIRECTOR,
CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES**

Mr. KUPPERMAN. Thank you for having me. I am especially pleased to appear before you. The subject of emergency management is long neglected, and there is no question that, in particular, informational technology can play an important role in improving our emergency preparedness.

We face the frequent problems of natural disasters—hurricanes, tornadoes, floods and earthquakes. Also, our civil defense program has been funded over many years to cope only with the threat of general nuclear warfare.

In fact, America's concern about coping with these calamities is not new. Most natural disasters are routine matters. Some, such as a California-style earthquake, pose truly significant managerial, technical and human problems. And the prospect of surviving general nuclear warfare is mindboggling. What is new, however, is the geopolitical environment which may bring terrorism to the United States of sufficient magnitude to tax our emergency management apparatus.

Moreover, environmental hazards, such as Love Canal, have become a serious national problem, so much so that an American city could face a toxic load equivalent to an incident of chemical warfare.

I am not an alarmist. However, when one combines the risks of natural disaster and increasing environmental hazards with the geopolitical and perceived domestic conditions which could bring terrorism to the United States, the likelihood of an especially unpleasant event is high enough to cause us to examine the state of our emergency planning.

While I have not followed the progress of the Federal Emergency Management Agency since the administration took office, as the former transition leader of FEMA, I was appalled by the state of America's emergency management apparatus. FEMA was less than 2 years old, though many of its components were the progeny of past bureaucracies. The agency was, in fact, a collection of aging entities clad in the emperor's new clothes.

Were the principal responsibilities of FEMA listed without the jargon of its organizational components, some of the functions vital to America's future would appear. The legislative intent behind FEMA and its predecessor agencies was to build a bridge between national security concerns and domestic emergency management. It appeared that we had lost the basic thrust, having buried FEMA in programs worn of age and museum pieces built of 20-year-old technology.

Put simply, the continuity of the Government program was outmoded and ineffective. Our capabilities to mobilize industry and to control the materials flow from the civilian economy to the mili-

tary were virtually nonexistent. Civil defense was not credible to the public, though it could be an integral part of our strategic policy.

Further, the management of terrorist incidents was alarmingly devoid of thought. And our planning to deal effectively with the trauma and relief phases of large scale disasters was minimal.

It would have been all too easy to leave FEMA alone, bury it, or in a fit of cathartic fervor, "blow it up." But such actions would have been temporarily therapeutic at best. I am encouraged that the commitment of the Reagan administration to national security will do much to reverse the erosion of our emergency management apparatus.

At times of calm, no one wishes to think of the disaster and contingency planning required to ameliorate human suffering and meet our security needs. But at times of stress, we invariably ask what happened to our emergency planning efforts.

Scapegoats are always sought and, as a consequence, some governmental relief is felt. Despite extraordinary efforts at denial, the problems of civil emergency preparedness will not go away.

We are prepared to handle only routine disasters—the small hurricane and the local flood. I am not trying to minimize the problem of the local police, fire, or other State or local officials facing such an issue but at a national level those are routine matters.

Yet, we speak glibly of our success at post nuclear attack recovery planning, when no American city is prepared to deal effectively with a large industrial accident, much less a California-style earthquake. We do business as usual by throwing money at the small disaster and fantasizing about our national capacity to cope with nuclear carnage.

It is time we face the realities of intermediate level disaster. What are we going to do if terrorists attack key nodes of the electrical power system, shutting off New York City's electricity for a month? What are the command, control and communication arrangements to deal with a cluster point of millions of people in need of shelter, food, physical protection, and hope? How are we to prepare for the truly large environmental accident? Have we developed the necessary Federal, State, and local management tools to cope at a technical, managerial, and human level?

Among the more difficult problems facing all levels of government during a disaster are the command, control, and communications considerations. For the case of the small disaster, time and money will heal the wounds caused by governmental incompetence.

However, no one seriously holds Government responsible for the near prompt restoration of society should a massive catastrophe befall the Nation. If, on the other hand, widespread flooding and damage would occur because of another Hurricane Agnes, or terrorists were to cause a large oilspill and fire in New York Harbor, all hell would break loose.

The Federal Government, as well as the State and local governments, would be clearly held responsible by an angry public.

My knowledge about our capacity to cope with such disasters is as current as the transition just prior to the time the administration took office. At that time, we were totally unprepared to con-

tend on an organizational or analytical level with such problems. There was no substantial crisis management apparatus. We were prepared as a government to act only in an ad hoc fashion.

All of the sophisticated management information systems and communication systems are for naught unless the senior most officials of government are willing to at least familiarize themselves with the sorts of decisions they may have to make. In this regard, I have urged repeatedly that a variety of simulations or exercises be conducted by operating and policy level personnel so that a variety of problems are presented that are typical of the situations which could confront government.

There have been many simulations dealing with total catastrophe some of which are to my mind exercises in fantasy. Also, there have been a number of exercises pertaining to hostages, but these tend to deal with little more than the tactical aspects of rescue.

In all cases, however, to my knowledge, the President and the Vice President, along with the senior Cabinet members have never participated in them. It is, therefore, impossible for the operating level of government to anticipate the problems confronting top-level policy management at times of genuine crisis.

There is no point in having a colonel play Secretary of Defense, the usual norm. At best, games, such as those played by the Studies and Analysis Gaming Agency, rarely capture more than an assistant secretary.

In August 1980, I designed and directed a crisis management game concerning terrorism. This involved a scenario in which a group highjacked an oil tanker and brought it within a few hundred yards of the World Trade Center in New York. We presented a very senior government team in the sense of the game with a variety of international, national, and local problems. Although it was a "game," a lot was learned. The American public saw the exercise on ABC television on August 6, 1981, and was given the opportunity to appreciate the shades of gray in a difficult decisional setting as well as the attendant command and control issues.

Among the top level personnel was Joseph Sisco, who played the National Security Adviser; John Lehman portrayed the Secretary of the Navy; and Ron Nessen acted the White House Press Secretary.

The Control Team also consisted of experienced individuals: Thomas Moorer as military adviser had been Chairman of the Joint Chiefs; Raphael Eitan, Prime Minister Begin's adviser on terrorism, acted as the Israeli Ambassador; and Frank Bolz, chief hostage negotiator for the New York City Police Department played himself.

From the show's reviews, it was evident that the critics found the content interesting. A few papers, the Washington Post, for example, objected to the airing of a show of this nature, while most of the others, including the Los Angeles Times, were quite supportive. There were comparatively few neutral or ambivalent references.

I feel that it is truly necessary to undertake a series of operational and policy-level simulations of disasters. We must analyze the crisis roles played at all levels of government to better understand

specific needs and to acquire efficient management techniques and relevant technology.

If such expertise can be developed by Federal, State, and local governments, it will go a long way toward preparing officials for the unexpected and reduce the risks for both the decisionmakers, and the general public as well.

[The prepared statement of Mr. Kupperman follows:]

PREPARED STATEMENT OF ROBERT H. KUPPERMAN

I am especially pleased to appear before you. The subject of emergency management is long neglected, and there is no question that, in particular, informational technology can play an important role in improving our emergency preparedness. We face the frequent problems of natural disasters—hurricanes, tornadoes, floods and earthquakes. Also our civil defense program has been funded over many years to cope only with the threat of general nuclear warfare.

In fact, America's concern about coping with these calamities is not new. Most natural disasters are routine matters. Some, such as a California-style earthquake, pose truly significant managerial, technical and human problems. And the prospect of surviving general nuclear warfare is mindboggling. What is new, however, is the geopolitical environment which may bring terrorism to the United States of sufficient magnitude to tax our emergency management apparatus. Moreover, environmental hazards, such as Love Canal, have become a serious national problem, so much so that an American city could face a toxic load equivalent to an incident of chemical warfare.

I am not an alarmist. However, when one combines the risks of natural disaster and increasing environmental hazards with the geopolitical and perceived domestic conditions which could bring terrorism to the United States, the likelihood of an especially unpleasant event is high enough to cause us to examine the state of our emergency planning.

While I have not followed the progress of the Federal Emergency Management Agency since the Administration took office, as the former transition leader of FEMA I was appalled by the state of America's emergency management apparatus. FEMA was less than two years old, though many of its components were the progeny of past bureaucracies. The Agency was, in fact, a collection of aging entities clad in the Emperor's new clothes.

Were the principal responsibilities of FEMA listed without the jargon of its organizational components, some of the functions vital to America's future would appear. The legislative intent behind FEMA and its predecessor agencies was to build a "bridge" between national security concerns and domestic emergency management. It appeared that we had lost the basic thrust, having buried FEMA in programs worn of age and museum pieces built of twenty year-old technology.

Put simply, the continuity of the government program was outmoded and ineffective. Our capabilities to mobilize industry and to control the materials flow from the civilian economy to the military were virtually nonexistent. Civil Defense was not credible to the public, though it could be an integral part of our strategic policy. Further, the management of terrorist incidents was alarmingly devoid of thought. And our planning to deal effectively with the trauma and relief phases of large scale disasters was minimal.

It would have been all too easy to leave FEMA alone, bury it, or in a fit of cathartic fervor, "blow it up." But such actions would have been temporarily therapeutic at best. I am encouraged that the commitment of the Reagan Administration to national security will do much to reverse the erosion of our emergency management apparatus.

At times of calm, no one wishes to think of the disaster and contingency planning required to ameliorate human suffering and meet our security needs. But at times of stress, we invariably ask what happened to our emergency planning efforts. Scapegoats are always sought and, as a consequence, some governmental relief is felt. Despite extraordinary efforts at denial, the problems of civil emergency preparedness will not go away.

We are prepared to handle only routine disasters—the small hurricane and the local flood. Yet, we speak glibly of our success at post nuclear attack recovery planning, when no American city is prepared to deal effectively with a large industrial accident, much less a California-style earthquake. We do business as usual by throwing money at the small disaster and fantasizing about our national capacity to cope with nuclear carnage.

It is time we face the realities of intermediate level disaster. What are we going to do if terrorists attack key nodes of the electrical power system, shutting off New York City's electricity for a month? What are the command, control and communication arrangements to deal with a cluster point of millions of people in need of shelter, food, physical protection, and hope? How are we to prepare for the truly large environmental accident? Have we developed the necessary federal, state and local management tools to cope at a technical, managerial, and human level?

Among the more difficult problems facing all levels of government during a disaster are the command, control and communications considerations. For the case of the small disaster, time and money will heal the wounds caused by governmental incompetence. However, no one seriously holds government responsible for the near prompt restoration of society should a massive catastrophe befall the nation. If, on the other hand, widespread flooding and damage would occur because of another Hurricane Agnes, or terrorists were to cause a large oil spill and fire in New York harbor, all hell would break loose. The federal government, as well as the state and local governments, would be clearly held responsible by an angry public.

My knowledge about our capacity to cope with such disasters is as current as the transition just prior to the time the Administration took office. At that time we were totally unprepared to contend on an organizational or analytical level with such problems. There was no substantial crisis management apparatus. We were prepared as a government to act only in an ad hoc fashion.

All of the sophisticated management information systems and communication systems are for naught unless the senior most officials of government are willing to at least familiarize themselves with the sorts of decisions they may have to make. In this regard, I have urged repeatedly that a variety of simulations or exercises be conducted by operating and policy level personnel so that a variety of problems are presented that are typical of the situations which could confront government.

There have been many simulations dealing with total catastrophe, some of which are to my mind exercises in fantasy. Also there have been a number of exercises pertaining to hostages, but these tend to deal with little more than the tactical aspects of rescue. In all cases, however, to my knowledge, the President and the Vice President, along with the senior Cabinet members have never participated in them. It is, therefore, impossible for the operating level of government to anticipate the problems confronting top-level policy management at times of genuine crisis. There is no point in having a Colonel play Secretary of Defense, the usual norm. At best games, such as those played by the Studies and Analysis Gaming Agency, rarely capture more than an assistant secretary.

In August, 1980, I designed and directed a crisis management game concerning terrorism. This involved a scenario in which a group hijacked an oil tanker and brought it within a few hundred yards of the World Trade Center in New York. We presented a very senior "government team" in the sense of the game with a variety of international, national, and local problems. Although it was a "game", a lot was learned. The American public saw the exercise on ABC Television on August 6, 1981, and was given the opportunity to appreciate the "shades of gray" in a difficult decisional setting as well as the attendant command and control issues.

Among the top level personnel was Joseph Sisco, who played the National Security Adviser; John Lehman portrayed the Secretary of the Navy; and Ron Nessen acted the White House Press Secretary. The Control Team also consisted of experienced individuals: Thomas Moorer as military adviser had been Chairman of the Joint Chiefs; Raphael Eitan, Prime Minister Begin's adviser on terrorism, acted as the Israeli ambassador; and Frank Bolz, Chief Hostage Negotiator for the New York City Police Department played himself.

From the show's reviews, it was evident that the critics found the content interesting. A few papers, the Washington Post, for example, objected to the airing of a show of this nature, while most of the others, including the Los Angeles Times, were quite supportive. There were comparatively few neutral or ambivalent references.

I feel that it is truly necessary to undertake a series of operational and policy-level simulations of disasters. We must analyze the crisis roles played at all levels of government to better understand specific needs and to acquire efficient management techniques and relevant technology. If such expertise can be developed by federal, state and local governments, it will go a long way toward preparing officials for the unexpected and reduce the risks for both the decisionmakers, and the general public as well.

Mr. GORE. Thank you. That is very impressive. I want to commend your exceedingly pragmatic approach to this whole subject. That is one of the reasons we chose you to be the concluding

witness in this 2-day hearing. I want to also commend the effort that you made with others during the transition period to focus attention on how much more can be done to make our emergency response capabilities what they should be.

The military routinely conducts what they refer to as command post exercises to test both commanders and their staffs and communications facilities and they usually involve scenarios almost as imaginative as the one you developed involving the World Trade Center.

Do you think FEMA should have similar exercises if they could be conducted in a way that did not inconvenience the communities involved?

Mr. KUPPERMAN. I feel strongly they must. If we are going to limit our thought processes to disasters that are fundamentally tractable—the small hurricane, the local flood as bad as it may be, where the trauma phase just passes and the Government—the Federal Government goes on and pays a share. You don't need such aids particularly. They may be helpful. Certainly, training aids are important and one should use FEMA's training institute and improve itself and enhance the Government's abilities.

On the other hand, if we go beyond the small hurricane problem, we are going to involve the National Government immediately. The operating level, even within the Federal Government, may well be ignored. I spent 6 years in the White House. It is absolutely clear to me that at a time of deep trouble the President—I am not picking on any one President—grabs his closest advisers who may know absolutely nothing about the crisis or, its resolution, simply for emotional support at the time. We need to get the Presidential advisers involved in exercises. We also need an operating means to in effect "convene" the principal operating level personnel FEMA is the bureaucratic device.

In this sense, I think such exercises are indispensable.

Mr. GORE. You mentioned this terrorism scenario. We like to think that is most improbable.

Mr. KUPPERMAN. I would as well.

Mr. GORE. But what do you think is the probability of some sort of incident?

Mr. KUPPERMAN. About one.

Mr. GORE. About one in one?

Mr. KUPPERMAN. Yes.

Mr. GORE. So, we might as well begin to prepare for managing some such threats in the future?

Mr. KUPPERMAN. Look, we have had situations of—I don't know the numbers, 80, 90, 100, whatever—nuclear weapons extortions that were nonsensical, people who have no knowledge of how to make a nuclear weapon; such as religious psychotics who were claiming all sorts of power but some were just criminal extortions.

One day we are going to face something real. One day we are going to face a biological incident that is real. It is happening now, and to claim the United States will remain forever immune is nonsensical and dangerous.

Mr. GORE. Well, that is not hard to understand. You put that very clearly. What would your recommendations be if you were in the place of this subcommittee making recommendations?

Mr. KUPPERMAN. I could not put myself in that place, but let me try anyway.

I think we need to create around the President a core crisis management mechanism, a small staff, derived from FEMA, that forces the Presidency—as distinguished from the President—into the business of periodically examining our contingency plans, periodically getting involved in exercises—at least observing them—in trying to choose what scenarios ought to be the exercised, and in convincing the Governors and the mayors of major cities that they should cooperate—that this is one nation and that there are substantial problems that will be felt by everyone if the level of disaster increases just slightly.

Mr. GORE. To narrow that recommendation a little bit, would you agree that it might make sense to recommend that the President designate a single person on the White House staff as liaison with FEMA, empowered to suggest exercises and scenarios to test and evaluate the information management groups and the requirements of decisionmakers on a regular basis.

Mr. KUPPERMAN. I think that would be very useful. I think the big problem is that the White House is beset by every imaginable problem every day. No White House in my view has a planning horizon beyond 10 minutes. It is simply always in trouble. It is suffering from a continuing paranoia and though you may designate somebody to do this, how do you keep that individual alive enough in the policy and bureaucratic setting of the White House to actually—take Ed Meese for example—to think about these issues.

While inherently that is a basic interest of his, it is just a resource problem that he and other major officials, the President included, must face in allocating their time.

It is a very difficult problem. It is easiest to attempt to put it off.

Mr. GORE. Well, I think we have an opportunity to get their attention in a way that greatly enhances the chances of this happening. So we will review what you have said here when we write the report.

In light of the time I think we are going to have to conclude but I would like to thank you again for an excellent presentation and for all the work you have done in this area. We may be back in touch with you as we get down to the work of the finishing up this report and the recommendations contained in it.

It has been an interesting 2 days and it has been interesting to listen to the various prospectives presented by all of our witnesses. I would like to thank all of them again and Dr. Kupperman, our thanks to you as well.

With that, the subcommittee will stand adjourned.

[Whereupon at 1:05 p.m. the subcommittee adjourned.]